HAL
open science

Cours Interconnexion et conception de réseaux (informatiques)

Jean-Luc Archimbaud

To cite this version:

Jean-Luc Archimbaud. Cours Interconnexion et conception de réseaux (informatiques). Engineering school. A Grenoble à l'ENSIMAG (cours donné 2 fois), 2002, pp.322. cel-00561873

HAL Id: cel-00561873

https://cel.hal.science/cel-00561873v1

Submitted on 2 Feb 2011

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Interconnexion et conception de réseaux

Cours de 24 h pour 3ième année
Ecole d'ingénieurs réseaux
2002

Jean-Luc Archimbaud CNRS/UREC

Interconnexion et conception de réseaux

- **Réseau :**
  - **Qu'est-ce ?**
  - **Plusieurs réseaux interconnectés ✍ réseau**
  - **Dans le cours : réseau informatique d'entreprise – de campus**
- **Concevoir un réseau c'est actuellement :**
  - **Faire évoluer l'existant**
  - **Réfléchir à toutes les couches**
    - Tranchées ✍ Applications
  - **Utiliser les services des opérateurs – sous-traitance**
  - **Travail de puzzle : assemblage de briques**
    - Matériel - logiciel

Concevoir un réseau c'est définir

- L'architecture physique (réseau = câble)
  - Carte des sites – bâtiments – salles à connecter
  - Les supports physiques
  - Les équipements actifs
- L'architecture logique (réseau = réseau IP)
  - Les protocoles
  - Plan adressage – Routage
- L'administration des équipements - surveillance
- Les services réseaux
  - DNS (nommage), Messagerie, Web, …
- Les outils de sécurité
- Les connexions avec l'extérieur : Internet, …

Adaptée aux équipements - besoins des utilisateurs

Stations – Serveurs – Applications

Plan du cours

- Réseaux locaux - LAN
  - Liens physiques - câblage : Coax - TP – FO – sans fil
  - Câblage de bâtiment
  - Protocoles niveau 1-2 : Ethernets – FDDI
- Rappels : caractéristiques du protocole IP
- Eléments actifs d'interconnexion Eth-IP
  - Répéteurs – hubs (Ethernet)
  - Ponts (Ethernet)
  - Commutateurs Ethernet
  - Routeurs (IP)
  - Commutateurs-routeurs (Ethernet-IP)

Plan du cours

- **Liaisons longues distances**
  - **Liaisons physiques**
    - Commutées RTC, RNIS, ADSL, X25, louées LS
  - **Modems**
- **ATM**
  - **Objectifs**
  - **QoS : Qualité de Service**
  - **Couches 1 et 2**
  - **Commutateurs et routage**
  - **Architectures LS et LANE**
  - **Bilan**
- **Exemples d'architecture**

Plan du cours

- **Architecture logique IP**
  - **Adresses IP**
  - **Plan adressage IP**
  - **Routage IP**
  - **Exemples de répartition d'utilisateurs et de services**
  - **Architecture ATM : classical IP**
- **MPLS**
- **Intégration voix-données (téléphonie – informatique)**
  - **Pourquoi ?**
  - **Différents niveaux d'intégration**
  - **Téléphonie sur IP**
    - Services rendus
    - H323
    - SIP
  - **Bilan aujourd'hui**

Plan du cours

- **Réseaux virtuels**
  - **Pourquoi ?**
  - **VLAN**
  - **Avec ATM**
  - **VPN (PPTP, L2TP, IPsec)**
- **Services d'interconnexion de France Télécom**
  - **Interconnexion niveau 2 moyen débit**
  - **Interconnexion niveau 2 haut-débit**
  - **Services (entreprises)**
- **Services à assurer – couche 7**
  - **Noms**
  - **Messagerie**
  - **Annuaire**
  - **Services Web**

Plan de cours

- **Qualité de service IP –rappels**
  - **RSVP**
  - **DiffServ**
- **Fonctions « annexes » de certains équipements actifs**
  - **Rappels**
  - **NAT**
  - **Filtrage**
  - **Multicast**
  - **Gestion des files d'attente**
- **Administration de réseau**
- **Quoi ?**
  - **Equipes, standards**
  - **Configuration, surveillance, dépannage**
  - **Stations d'administration**
  - **Métrologie**

Plan du cours

- **Quelques éléments de sécurité**
- **Accès à l'Internet**
- **Accès depuis l'Internet**
  - **A l'Intranet**
  - **Aux serveurs Internet**
- **Construction d'un réseau « solide »**
- **Etudes de cas**
  - **Réseau de petit laboratoire éclaté**
  - **Réseau de campus**
    - Gros site d'une entreprise
  - **Réseau Renater (national)**
    - Entreprise multi-sites

Bibliographie

- **Computer Networks 3rd edition (Tanenbaum)**
- **TCP/IP Illustrated, Vol 1 - W. Richard Stevens**
- **Constructeurs (white papers)**
  - **CISCO : http://www.cisco.com**
  - **…**
- **Elements d'interconnexion Ethernet**
  - **http://www.unige.ch/dinf/jfl/elem/index.htm**
- **Pointeurs cours, mémoires**
  - **http://reseau.plisson.org/**
- **Cours UREC**
  - **http://www.urec.cnrs.fr/cours/**
- **Moteurs de recherche**

LAN : dimension

- **LAN : Local Area Network**
  - **Un étage**
  - **Un bâtiment**
  - **Diamètre < 2 km**
  - **Un site géographique : domaine privé**
  - **Plusieurs bâtiments (site-campus)**
    - Interconnexion de LAN
- **MAN : Metropolitan Area Network**
  - **Dimension d'une ville**
  - **Diamètre < 10 km**
  - **Domaine public : service d'opérateurs locaux**
- **WAN : Wide Area Network**
  - **Très longues distances : opérateurs (inter)nationaux**

LAN : Liens physiques : critères choix

- **En théorie : propriétés physiques**
- **En pratique :**
  - **Coût**
    - Câble (media)
    - Connecteurs (connectique)
    - Emetteurs et récepteurs
    - Installation : pose (tirer des câbles)
  - **Immunité aux perturbations**
    - Foudre, électromagnétiques, …
  - **Longueur maximum possible entre deux équipements actifs (✍ minimiser le nb)**
    - Coût équipement
    - Besoin alimentation électrique, …
  - **Débits possibles (surtout débit max) : bps**

LAN : liens physiques : câble coaxial

- **Bande de base : Baseband**
  - **50 ohm – transmissions numériques – quelques kms**
  - **Ex : Ethernet câble jaune – bus - prises vampires - 10base5 (500 m)**
- **Large bande : Broadband (LAN, MAN, WAN)**
  - **75 ohm – transmissions analogiques – 100 kms**
  - **Plusieurs bandes de fréquences ✍ plusieurs flux**
  - **Ex : câble télévision**
- **Bons débits (Gbits/s) et distances, bonne immunité**
- **Problème : cher**
  - **Equipements - encombrement (Ø = 1 cm)– difficulté de la pose**
- **N'est plus utilisé pour le LAN informatique**
  - **Il peut rester quelques câbles coaxiaux jaunes Ethernet et Ethernet fin (Bande de base) : 10base2 (185 m) - Prises en T**
- **Utilisé dans le réseau câble des villes**
  - **Connexion ordinateur : Carte 10BaseT – Modem – Câble (TV)**

LAN : câble coaxial fin et prise en T

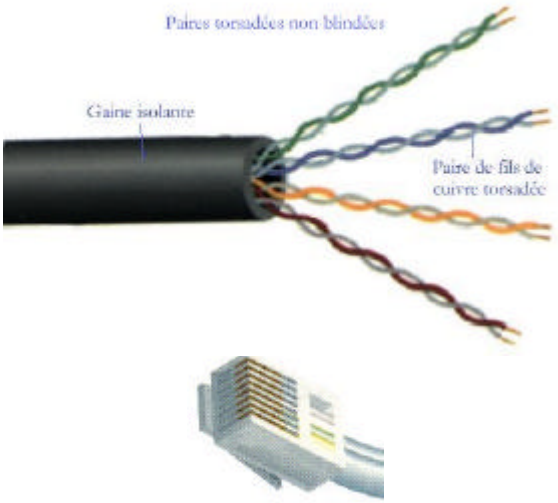
LAN : Liens physiques : TP

- **TP : Twisted Pair : Paire torsadée**
- **Fil de cuivre isolé de diamètre 1 mm**
- **Utilisé depuis très longtemps pour le téléphone**
- **TP catégorie (type de TP mais aussi composants)**
  - **3 : jusqu'à 16 Mhz : très répandu aux USA**
  - **4 : jusqu'à 20 Mhz : peu utilisé**
  - **5 : jusqu'à 125 Mhz : le plus répandu actuellement**
    - Câbles 4 paires avec des pas de torsades différents
  - **5E : amélioration du câblage 5 (Gigabit Ethernet)**
  - **6 : jusqu'à 250 Mhz**
  - **7 : jusqu'à 600 Mhz**
- **Blindage des câbles :**
  - **UTP : Unshielded : pas de blindage**
  - **STP : Shielded : blindage avec tresse métallique**
  - **FTP : Foiled : entourée d'un feuillard d'aluminium**

LAN : Liens physiques : TP

- **Nombre de paires utilisées : 2 à 4 suivant l'utilisation**
- **Connexions point à point : architecture en étoile**
- **Connecteurs RJ45 : 4 paires**
- **Avantages :**
  - **Câblage universel : informatique et téléphone**
  - **Débit : plusieurs Mbits/s et Gbits/s sur 100 m (jusqu'à quelques centaines)**
  - **Câble et pose peu chers**
- **Désavantages :**
  - **Très sensibles aux perturbations (électromagnétiques, …)**
  - **Courtes distances**
  - **Beaucoup de câbles : pose par professionnels**
- **C'est le media le plus utilisé à l'intérieur des bâtiments**

LAN : photos TP et RJ45



LAN : Liens physiques : FO

- **FO : Fiber Optic : Fibre Optique**
- **2 types : multimode - monomode**
  - **Multimode : rayons lumineux avec réflexions : dispersion**
    - Cœur optique : diamètre 50 ou 62.5 microns
    - Gaine optique : 125 microns
    - Multimode 50 ou 62.5 (le plus courant aujourd'hui)
  - **Monomode (single mode) : rayons lumineux « en ligne droite »**
    - Cœur optique avec un diamètre plus petit : 9 microns
    - Gaine optique : 125 microns
  - **Monomode pour de plus longues distances et plus haut débits**
- **Plusieurs fenêtres de longueurs d'onde possibles pour le faisceau lumineux émis**
  - **Fenêtres d'émission centrées sur : 850, 1300 et 1550 nm**

LAN : Liens physiques : FO

- **Connectique :**
  - **Epissures (définitif) ~ soudures**
  - **Connecteurs : les plus répandus : SC (encliquetage) et ST (baionnette)**
- **Emetteurs :**
  - **Photodiodes (LED) : multimode, débits moyens, distances courtes-moyennes, peu chers**
  - **Lasers : multi ou monomode, très hauts débits, longues distances, plus chers**
  - **Plus faciles à installer sur de la fibre multimode**
- **Unidirectionnel : 2 FO pour une liaison**
- **Câbles généralement de 2 à 40 fibres**

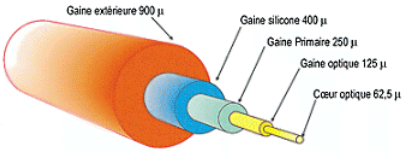
LAN : Liens physiques : FO

- **Budget optique :**
  - **Emetteur-récepteur : quelle « atténuation optique » maximale possible peut-on avoir ?**
    - Ex 12 dB
  - **Affaiblissements dans chaque liaison**
    - Distance : lg de fibre : 3.5 dB/km pour FO 62.5 - 850 nm
    - Connectique : épissure : 0.2 dB, connecteur : 2 dB, …
    - Détérioration des éléments
  - **Affaiblissement total de la liaison < budget optique**
- **Multiplexage optique**
  - **Multiples longueurs d'ondes sur une même fibre**
  - **Protocole DWDM (Dense Wavelengh Division Multiplexing)**
  - **Mutiplexeurs, démultiplexeurs, commutateurs optiques**
  - **Choix n fibres ou multiplexage optique : coût**

LAN : Liens physiques : FO

- **Avantages-inconvénients**
  - **Débits possibles très élevés (potentiellement immenses)**
  - **Longues distances (dizaines voir centaines de km)**
  - **Insensible aux perturbations électromagnétiques**
  - **… confidentialité**
- **Utilisation**
  - **C'est le support maintenant le plus utilisé en interconnexion de bâtiments, en MAN et WAN**
  - **Quelques fois en câblage de stations : cher**

LAN : photos de FO et connecteurs



Connecteur SC

Connecteur ST

LAN : sans fil

Liaisons radio LAN (R-LAN - WIFI) : 2.4 GHz

- **Architecture étoile**
  - **Carte sur stations (PC, …) avec antenne**
  - **Concentrateur avec antenne : borne**
    - Connecté au réseau câblé : borne
- **Normes IEEE 802.11**
    - Même rôle que 802.3 pour Ethernet
- **Distance max station-borne : entre 50 et 200 m**
- **Débits max**
    - 11 Mbits/s partagés (802.11b) : 10 M à 10 m, 1 M à 50 m
    - Evolutions : Jusqu'à 54 Mbps (802.11a), 20 Mbps et + (802.11g)

LAN : R-LAN

- **Utilisation : intérieur de bâtiment (en R-LAN)**
  - **Liaisons provisoires : portables, conférences, …**
  - **Locaux anciens et protégés (impossible d'effectuer un câblage)**
- **Problèmes**
  - **Débit limité**
  - **Sécurité : diffusion**
    - Contrôle de l'espace de diffusion
    - WEP (Wired Equivalent Privacy)
    - Fixe les adresses Ethernet
    - Considère comme « externe » : ajout IPSec, …
- **Se déploie très fortement actuellement**
- **MAN aussi : boucle locale radio (BLR 8M)**

LAN : sans fil

Liaisons laser

- **Depuis de nombreuses années**
- **Point à point : interconnexion de réseaux**
- **Distance : 1 ou 2 km sans obstacle**
- **Débits : plusieurs Mbits/s**
- **Utilisation :**
  - **Quand coût tranchées trop élevé ou domaine public**
  - **Liaison provisoire**
- **Problème : réglage de la direction du faisceau**

LAN-MAN : sans fil

- **Faisceaux hertziens : de 2.4 à 40 GHz**
  - **Pas les mêmes fréquences que R-LAN**
  - **Demande une licence à l'ART et une redevance**
  - **Maxima de débit : de l'ordre de**
    - 2 - 34 voir 155 Mbits/s jusqu'à plusieurs km
  - **Interconnexion de réseaux (et téléphone)**
  - **Utilisation :**
    - Plutôt en MAN
    - Demande une solide étude préalable (obstacles …)
    - Interconnexion de sites distants sans besoin d'opérateur
    - Utilisé par les opérateurs (France Télécom …)
- **Satellite : pas en LAN !**
  - **Service d'opérateur**
  - **Quand FO non disponible**

LAN : câblage de bâtiment (TP)

(vocabulaire)

- **Construction d'un bâtiment : pré-câblage**
- **TP : câblage courants faibles : informatique et téléphone**
- **Répartiteur : local technique**
  - **Nœud de concentration et de brassage**
  - **Arrivées-départ des liaisons, équipements actifs**
- **Dans un grand bâtiment**
  - **1 répartiteur général : RG**
  - **n sous-répartiteurs : SR**
  - **Entre RG et SR : câblage primaire : rocades ou colonnes**
  - **Entre SR et prises stations : câblage horizontal**
  - **Structure étoilée**
- **Câbles - connecteurs – cordons - jarretières – baies de brassage**

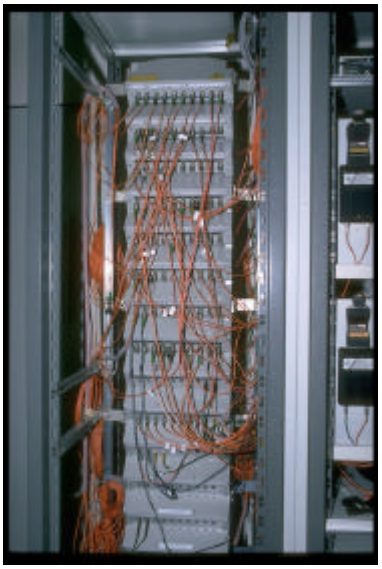
LAN : câblage de bâtiment (TP)

- **Chemins de câbles :**
  - **gaines techniques**
  - **faux plafond**
  - **goulottes, …**
- **Bureaux :**
  - **Prises murales**
  - **Recommandation CNRS : 3 prises (tél + info) par personne**
- **Tests après installation : cahier de recette**
  - **Certification (classe d'installation : classe D)**
  - **Réflectométrie**
  - **Etiquetage – plans : obligatoire**
    - Base de données pour le système de câblage ?
- **Travail de spécialistes**

Sans bon câblage, pas de bons services
Câblage : fondations du réseau

LAN : Photo baie de brassage optique

–

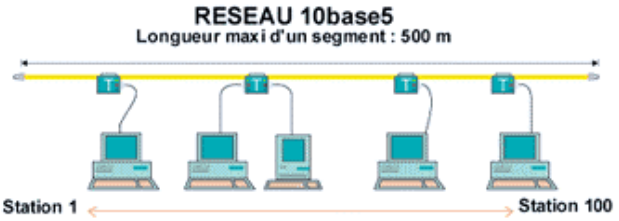


LAN : tous les Ethernets

- **Protocoles pour LAN (au départ)**
  - **Gigabit Eth : protocole différent (sauf trame) ✍ MAN**
- **Trame**
  - **Adresse destination (MAC address) : 6 octets 08:00:20:06:D4:E8**
  - **Adresse origine (MAC address) : 6 octets**
  - **Type (IP = 0800) ou longueur (IEEE 802.3) : 2 octets**
  - **Données : taille variable < 1500 octets**
- **Adresses (6 bytes) – MAC address**
  - **Station : unique**
    - 3 premiers octets : constructeur
      - CISCO 00:00:0C
      - Sun 08:00:20
      - HP 08:00:09
    - 3 octets suivants : coupleur
  - **Broadcast : FF:FF:FF:FF:FF:FF**
  - **Multicast : 1er octet impair**

LAN : Ethernet 10 M - 10Base5

- Protocole : Ethernet – IEEE802.3
- Début 1980
- Conçu pour 10Base5 : bus : coaxial : diffusion
- Méthode d'accès : CSMA-CD
  - Carrier Sense Multiple Access-Collision Detection
  - Accès multiple et écoute de porteuse – Détection de collision



LAN : Ethernet 10 M - 10Base5

- 10 Mbits/s (partagés)
- CSMA-CD :
  - Emet quand le media est libre
  - Si autre signal sur le media durant émission : arrête l'émission
- RTD : round trip delay < 51.2 µs ✍ lg max réseau
- Taille minimum trame envoyée (correcte) : 64 bytes
- Quand trame taille < 64 bytes : collision
- 10Base5 : 5 câbles 500 m avec répéteurs : 2.5 km
- Problèmes 10Base5
  - Coût : câble et connectique
  - Sensibilité aux perturbations électromagnétiques
  - Besoin d'une même terre
- Solution bas prix : 10Base2
  - Thin Ethernet - 185 m - stations en coupure
- 10Base5 et 10Base2 ✍ 10BaseT

LAN : Ethernet 10 M - 10BaseT

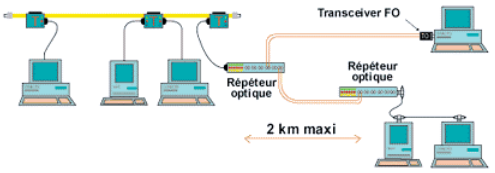
- CSMA-CD, 10 Mbits/s, RTD < 51.2 µs
- Câble : paire torsadée : UTP 5 – RJ45
- Architecture étoile : centre : hub (multi-répéteur)
- Distance max hub-station ou hub-hub : 100 m
- 4 hubs max entre 2 stations : 500 m lg max

RESEAU 10baseT

LAN : Ethernet 10 M : 10BaseF

- Pbs 10BaseT : perturbations – distance
  - ✍ 10BaseF
- CSMA-CD, 10 Mbps, RTD < 51.2 µs
- Liaison : 2 FO multimode 50 ou 62.5
- Connecteurs SC ou ST
- Station – Répéteur : 1 km
- Répéteur

LIAISON PAR FIBRE OPITQUE



LAN : Ethernet 10 M

- **Réseau au sens Ethernet : domaine de broadcast**
- **Avantage : protocole simple**
- **Problèmes :**
  - **Débit limité (10 M partagé)**
  - **Distances limitées**
  - **Dépendance vis a vis de son voisin (collisions, charge)**
  - **Broadcast : charge**
  - **Pas de confidentialité (diffusion)**

LAN : Ethernet 100 M – 1000 M

- **100BaseT (IEEE802.3U) – Fast Ethernet 1995**
  - **Idem 10BaseT (CSMA/CD, RJ45, …)**
    avec débit x 10 et taille réseau / 10
  - **TP (100BaseT) ou FO (100BaseF)**
  - **Distance max : Hub – Station : 100 m (TP) - 412 m (FO)**
  - **Lg max réseau 100BaseTX : 250 m**
  - **Utilisation : serveurs ✍ stations**
  - **Auto-négociation débit : 10 ou 100**
- **1000Base – Gigabit Ethernet**
  - **Idem 100Base avec débit x 10 – Taille min trame : 512 bytes**
  - **Câblage FO ou TP de très bonne qualité**
  - **Point à point, pas de diffusion**
  - **Full duplex possible**
  - **Utilisation : Serveurs - Backbone Campus – MAN**

ATTENTION : toutes les distances max Ethernet citées : réseau uniquement avec répéteurs-hubs

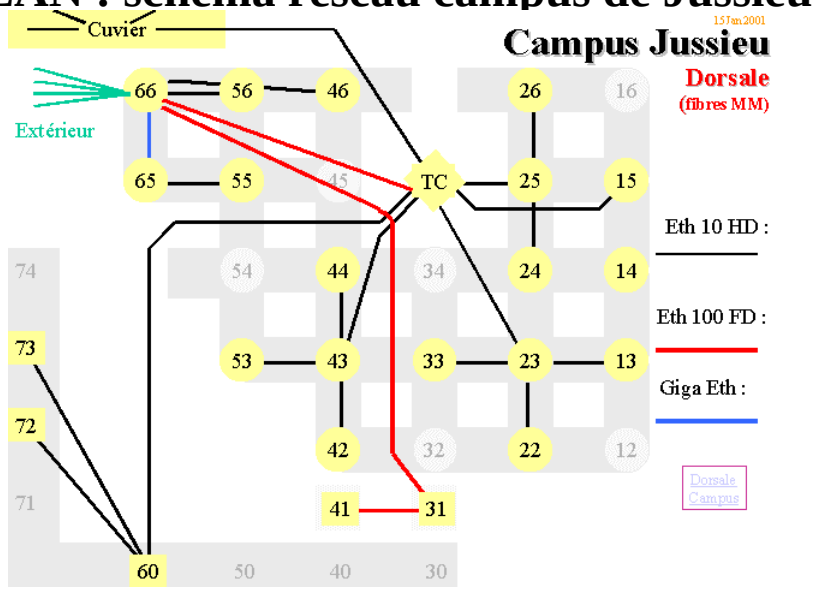
LAN : Ethernets

- **10Base5**
  - **10 Mbits/s - Coax jaune - Lg max rép – station : 500 m**
- **10Base2**
  - **10 Mbits/s – Coax fin – Lg max rép – station : 185 m**
- **10BaseT (IEEE802.3 – 1990)**
  - **10 Mbits/s – 2 paires UTP – Lg max hub-station : 100 m**
  - **1 paire pour chaque sens de transmission**
- **10BaseFL**
  - **10 Mbits/s – 2 FO (1 pour chaque sens)**
  - **Lg max rép et/ou stations : 2 km avec multimode 62.5**
- **100BaseTX**
  - **100Mbits/s - 2 paires UTP catégorie 5**
  - **Lg max hub-station : 100 m (réseau 250 m)**
- **100BaseT4 (peu utilisé)**
  - **100Mbits/s - 4 paires UTP Catégorie 3 ou 4**
  - **Lg max hub-station : 100 m (réseau 250 m)**

LAN : Ethernets

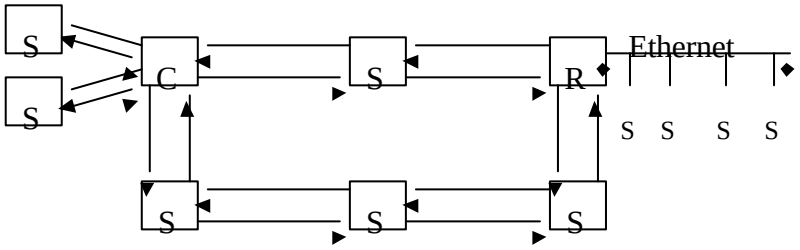
- **100 BaseFX**
  - **100 Mbits/s – 2 FO**
  - **412 m (HD) ou 2 km (FD) multimode 62.5**
  - **20 km monomode**
- **1000BaseSX (IEEE802.3z)**
  - **Sur 2 FO avec longueurs d'onde 850 nm**
  - **Lg max : multimode 50 550 m – 62.5 220 m**
- **1000BaseLX (IEEE802.3z)**
  - **Sur 2 FO avec longueurs d'onde 1300 nm**
  - **Lg max : multimode 50 550 m - monomode 5 km et plus**
- **1000BaseT (IEEE802.3ab – 1999)**
  - **Sur 4 paires UTP Cat 5E**
  - **Longueur max 100 m**

LAN : schéma réseau campus de Jussieu



LAN : FDDI

- **FDDI : Fiber Distributed Data Interface**
- **Protocole pour réseau local informatique**
- **Débit 100 Mbits/s (partagé)**
- **Anneau 2 FO multimode**
- **Nœud : station (SA/ DA)-concentrateur-routeur**
- **Réseau max : taille 100 km, 500 stations**



LAN : FDDI

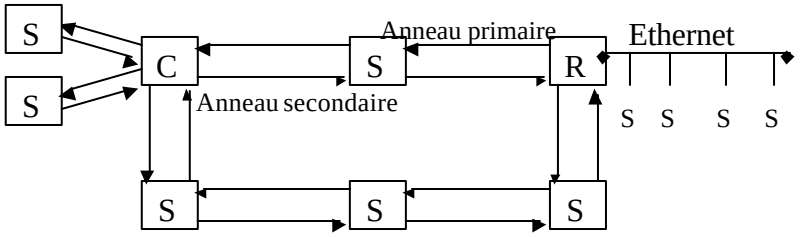
- **Accès au support par jeton (3 octets)**
- **Un jeton circule sur l'anneau**
- **Une station qui veut émettre**
  - **Capture le jeton**
  - **Envoie les trames de données**
  - **Libère le jeton**
  - **Retire ses trames au passage suivant**
- **Une station réceptrice**
  - **Lit les trames qui lui sont adressées**
  - **Modifie un champ des trames (FS) pour indiquer qu'elle a lu la trame**

LAN : FDDI

- **Trame**
  - **Adresse destination (6 octets idem Ethernet)**
  - **Adresse source**
  - **FS (Frame Status)**
    - Erreur
    - Adresse reconnue
    - Trame lue
  - **…**
  - **Données : lg max 4500 octets**
- **Pb : station FDDI ✍ station Ethernet**
  - **Taille des trames FDDI jusqu'à 4500 bytes alors que max Ethernet est 1500**
  - **Solution pour IP : fragmentation IP**

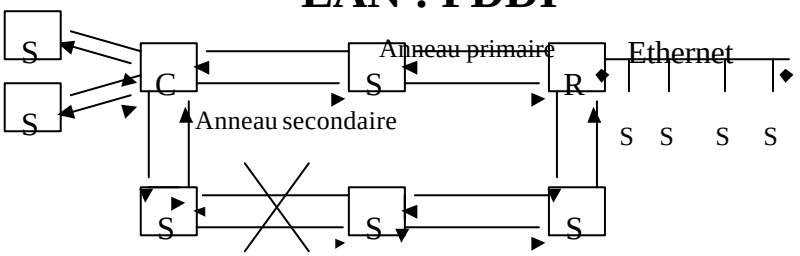
LAN : FDDI

- **Circulation normale : anneau primaire**
- **Coupure anneau**
  - **Rebouclage de l'anneau**
  - **Mise en fonction : anneau secondaire**

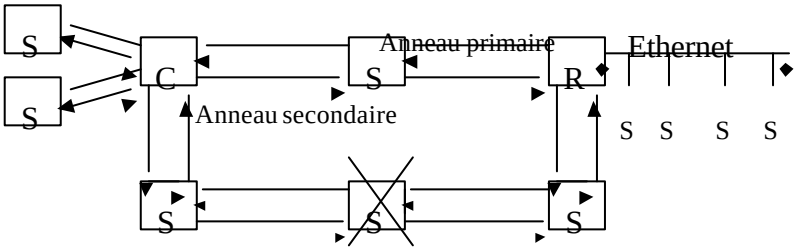


Fonctionnement normal

LAN : FDDI

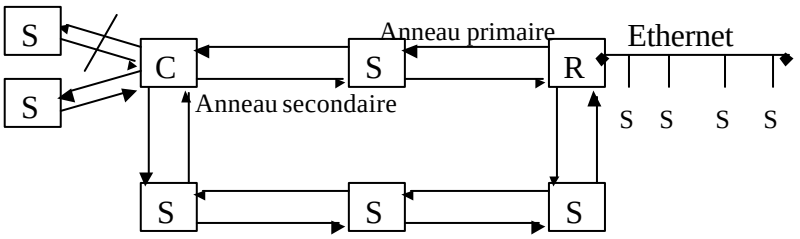


Coupure de lien



Arrêt de station

LAN : FDDI



Coupure lien station simple attachement

Possibilité d'avoir des stations prioritaires

CDDI : FDDI sur paire torsadée

Bilan :

FDDI trop cher – pas assez de débit

Maintenant remplacé par Ethernet 100 ou Giga

Bon example de réseau anneau à jeton

Rappels : caractéristiques IPv4

- **Protocole réseau : couche 3**
- **Mode non connecté**
- **Eléments d'un réseau IP :**
  - **Stations, réseaux (sens niv2), routeurs**
- **Informations : datagrammes (paquets)**
- **Entête datagramme :**
  - **Version (4)**
  - **TOS Type of Service : qualité de service**
  - **TTL Time To Live : 60 ✍ 0 (-1 à chaque routeur)**
  - **Identification protocole de transport (TCP, UDP, ICMP, …)**
  - **Adresse IP de la station origine**
  - **Adresse IP de la station destinataire**
  - **…**
- **Taille datagramme < 64 Koctets**
  Souvent de taille d'environ 512 ou 576 bytes

IPv4 : couche 4

- Couche 4 :protocole entre stations (pas entre routeurs)
- TCP : Transmission Control Protocol
  - Paquet TCP = segment
  - Mode connecté
  - Transport fiable (contrôle d'erreurs, accusés de réception, retransmission, …)
  - Spécification des applications : numéros de port (origine, destination) dans le segment
  - Fenêtrage – Slow start : s'adapte à tous les débits
- UDP : User Datagramm Protocol
  - Pas de contrôle
  - Mode non connecté
  - Spécification de l'application : numéros de port (orig, dest)
  - Protocole léger, permet multicast-broadcast facilement

IPv4 : ICMP

- ICMP : Internet Control Message Protocol
- RFC792
- Messages 'de contrôle' émis par les stations ou les routeurs
- Messages :
  - Ralentir le débit d'émission
  - Destination inaccessible
  - Demande d'echo
  - Réponse echo
  - « Time To Live » exceeded
  - Redirection
  - ….

IPv4 : couche 2

- **IP / couche 2 : les datagrammes IP peuvent être transportés par tous les types de réseaux :**
  - **Ethernet RFC894 et RFC1042**
  - **Liaison série : point à point (PPP RFC1331-1332)**
  - **ATM (RFC1577)**
  - **FDDI**
  - **X25**
  - **…**
- **@ IP ✍ @ couche 2 ?**
  - **Ethernet, FDDI : broadcast : ARP, RARP**
  - **ATM : serveur ARP**

IPv4 : exemple trame Ethernet (TCP)

Une trame Ethernet avec un segment TCP a la forme :

- **Entête Ethernet**
  - **@ Ethernet destination**
  - **@ Ethernet origine**
  - **Type = 800**
- **Entête IP**
  - **…**
  - **Indication TCP**
  - **@ IP origine**
  - **@ IP destination**
  - **…**
- **Entête TCP**
  - **Numéro de port source**
  - **Numéro de port destination**
  - **…**
- **Données**

IPv4 : adresses

- 4 bytes 194.220.156.3
- Chaque coupleur de station ou de routeur a une adresse
- Partie réseau (IP) : 194.220.156
- Partie station (IP) : 3
- Routeur : sépare (interconnecte) 2 réseaux IP
- Adresses (IP) de broadcast et de multicast
  - 194.220.157.255 : broadcast sur réseau IP 194.220.157.0
- Détails dans les cours suivants

Eléments d'interconnexion

Ethernet - IP

- Pourquoi ? – Problèmes
- Répéteurs – Hubs (Ethernet)
- Ponts (Ethernet)
- Commutateurs Ethernet
- Routeurs (IP)
- Commutateurs-Routeurs (Ethernet-IP)

Eléments d'interconnexion : pourquoi ?

- **Ré-amplifier les signaux**
  - **Electriques - optiques**
  - ✍ **Augmenter la distance maximale entre 2 stations**
- **Connecter des réseaux différents**
  - **Supports : Coax, TP, FO, Radio, Hertzien, …**
  - **Protocoles niveau 2 : Ethernet, FDDI, ATM, … rieur**
- **« Limiter » la diffusion (Ethernet)**
  - **Diminuer la charge globale**
    - Limiter les broadcast-multicast Ethernet (inutiles)
  - **Diminuer la charge entre stations**
    - Limiter la dépendance / charge des voisins
    - Objectif in fine : garantir une bande passante disponible (une qualité de service) entre 2 stations
  - **Limiter les problèmes de sécurité**
    - Diffusion ✍ écoute possible : pas de confidentialité

Eléments d'interconnexion : pourquoi ?

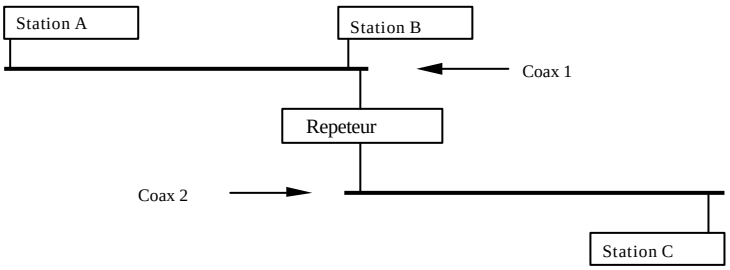
- **Restreindre le périmètre de la connectivité désirée**
  - **Extérieur ✍ Intérieur : protection contre attaques (sécurité)**
  - **Intérieur ✍ Extérieur : droits de connexion limités**
- **Segmenter le réseau :**
  - **Un sous-réseau / groupe d'utilisateurs : entreprises, directions, services, …)**
  - **Séparer l'administration de chaque réseau**
  - **Créer des réseaux réseaux virtuels**
    - S'affranchir de la contrainte géographique
- **Pouvoir choisir des chemins différents dans le transport des données entre 2 points**
  - **Autoriser ou interdire d'emprunter certains réseaux ou liaisons à certains trafic**

Eléments d'interconnexion : problèmes

- **Eléments conçus pour répondre a des besoins :**
  - **Qui ont évolué au cours du temps**
    - Durée de vie courte des équipements
    - Toujours mieux et moins cher
  - **Rapidement à moindre coût : pragmatique**
    - Chaque élément offre certaines fonctions les « prioritaires » du marché de l'époque
- ✍ **Problèmes :**
  - **Classification, frontières sont un peu complexes**
  - **Terminologie imprécise (dépend du contexte)**
    - Commerciaux rarement techniciens
- **Attention : le choix est un compromis entre les fonctions désirées et le coût**

Eléments d'interconnexion : répéteur

- **Répéteur (Ethernet)**
  - **Boite noire dédiée**
  - **Remise en forme, ré-amplification des signaux (électroniques ou optiques)**
  - **But augmenter la taille du réseau (au sens Ethernet)**
    - Exemple : distance max entre stations A - C : 500 m ✍ 1000 m

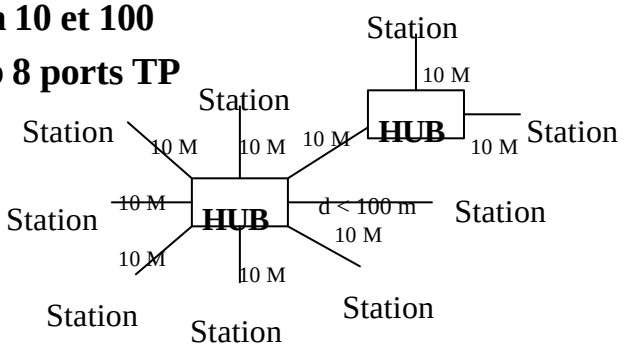


Eléments d’interconnexion : répéteur

- **Travaille au niveau de la couche 1**
- **Ne regarde pas le contenu de la trame**
- **Il n'a pas d'adresse Ethernet**
  - **Transparent pour les stations Ethernet**
- **Entre supports coaxiaux, TP et FO**
- **Avantages**
  - **débit 10 Mb/s**
  - **pas (ou très peu) d'administration**
- **Désavantages**
  - **Ne diminue pas la charge**
  - **Ne filtre pas les collisions**
  - **N’augmente pas la bande passante**
  - **Pas de possibilité de réseau virtuel (VLAN)**

Eléments d’interconnexion : hub

- **Hub : muti-répéteur : étoile (obligatoire TP)**
- **Idem répéteur pour :**
  - **Fonctions, avantages, désavantages**
- **Pour Eth 10 et 100**
- **Ex : Hub 8 ports TP**

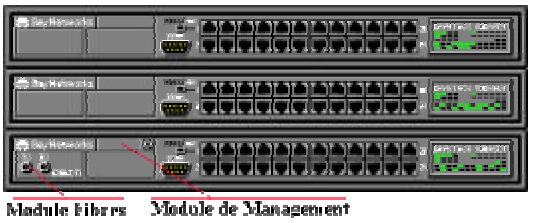


Eléments d'interconnexion : hub

- **Fonction annexes :**
  - **Affectation d'une @ MAC (@ Eth) à chaque brin : sécurité**
  - **« Auto-negotiation » débit hub 10-100 (IEEE 802.3u)**
  - **Surveillance SNMP**
- **Nombre maximum sur réseau Ethernet**
  - **10Base5 : 4 répéteurs**
  - **10BaseT : 4 hubs**
    - Distance max entre 2 stations : 500 m
  - **100BaseT : 4 hubs**
    - Mais distance max entre 2 stations : 250 m
  - **1000BaseX : utilise des commutateurs**
- **Utilisation actuelle**
  - **En « extrémité » de réseau (stations utilisateurs)**
  - **Remplacés par des commutateurs Ethernet**
    - En cœur de réseau, pour serveurs, et même pour stations

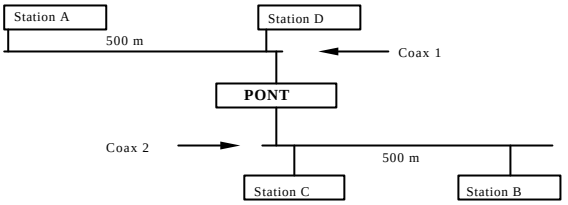
Eléments d'interconnexion :hub

- **Remarque : borne sans fil 802.11b = hub**
- **Face arrière hub stackable**
  - **3 x 24 ports TP (prises RJ45)**
  - **1 port FO (2 FO)**



Elts d'interconnexion : pont (Ethernet)

- **Aussi appelé répéteur filtrant ou "bridge"**



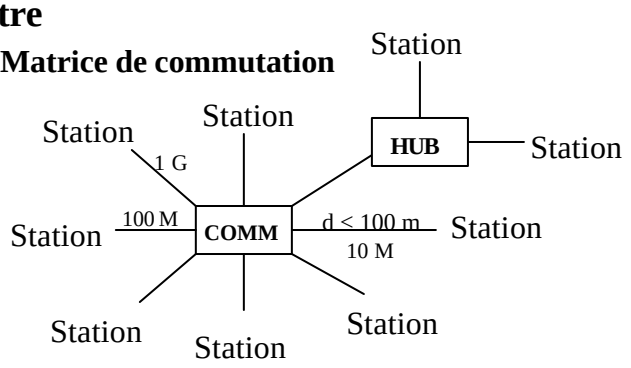
- **Niveau de la couche 2**
  - **Traitement : valeur @ MAC destinataire ✍ transmet ou non : trafic A-D ne va pas sur coax 2**
  - **Localisation des @ MAC des stations par écoute (auto-learning) ou fixée**
  - **Ignoré des stations (transparent)**

Elts d'interconnexion : pont

- **Avantages**
  - **Augmente la distance max entre 2 stations Ethernet**
  - **Diminue la charge des réseaux et limite les collisions**
    - Le trafic entre A et D ne va pas sur Coax 2
- **Remplacés en LAN par les commutateurs**
- **Fonctions supplémentaires : cf commutateurs**
- **Ponts distants**
  - **Ethernet – Liaison spécialisée (cuivre ou hertzienne ou laser)**
  - **Encore utilisés**

Elts d'interconnexion : commutateur

- **Commutateur – Switch Ethernet de niveau 2**
  - **10, 100, 1000 Mb/s TP ou FO**
- **Fonction : multi-ponts, cœur d'étoile**
- **Commute les trames Ethernet sur un port ou un autre**
  - **Matrice de commutation**



Elts d'interconnexion : commutateur

- **Mêmes fonctions et avantages que le pont + augmentation de la bande passante disponible**
- **Matériels - logiciel**
  - **Chassis ou boitier**
  - **Cartes : 2 ports FO, 8 ports TP … avec débits 10, 100, 1000 Mb/s**
  - **Système d'exploitation**
  - **Configuration : telnet, client Web**
  - **Surveillance : SNMP**
- **Quelques critères de choix techniques (performances)**
  - **Bus interne avec un débit max : 10 Gb/s**
  - **Vitesse de commutation nb de trames / s**
  - **Bande passante « annoncée » : 24 Gb/s**
  - **Nb d'adresses MAC mémorisable / interface**

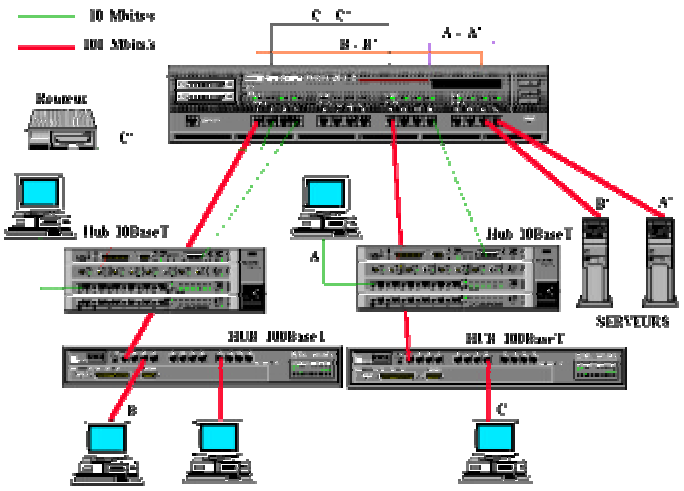
Elts d'interconnexion : commutateur

- **Permet : Ethernet Full duplex (TP ou FO)**
  - **Emission et réception en même temps : 2x10 ou 2x100**
  - **« Auto-negotiation » possible (IEEE 802.3u)**
- **Fonctions supplémentaires**
  - **Auto-sensing débit (IEEE 802.3u)**
  - **Affectation statique d'@ MAC et filtrage au niveau 2**
  - **Spanning Tree : évite les boucles**
    - Construction d'un arbre
    - A un instant : un seul chemin utilisé
  - **Réseaux virtuels : VLAN**
  - **Port d'écoute qui reçoit tout le trafic des autres ports**
    - Analyseur

Elts d'interconnexion : commutateur

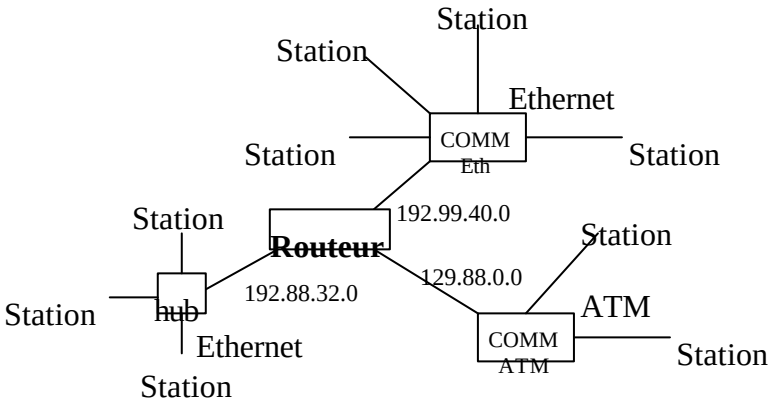
- **Limitations d'un réseau de commutateurs**
  - **Théoriquement pas de distance maximum**
  - **Broadcast et multicast diffusés partout**
  - **1 seul réseau IP possible**
- **Très répandu :**
  - **Local : workgroup switch**
  - **Campus : complété par le routeur (plus « lent » et plus cher)**
  - **Remplacé par le commutateur-routeur (plus cher) quand besoin**

Elts interconnexion : commutateur et hubs



Elts interconnexion : routeur (IP)

- **Niveau 3 : aussi appelé commutateur niveau 3**
  - **Il y a des routeurs multi-protocoles**
    - On ne parlera que de IP
  - **Interconnecte 2 ou plus réseaux (ou sous-réseaux) IP**



Elts interconnexion : routeur (IP)

- **Table de routage / @ IP destination**
- **N'est pas transparent pour les stations**
  - **Chaque station doit connaître l'@ IP du coupleur du routeur pour « le traverser »**
- **Pour le protocole Ethernet**
  - **C'est une station Ethernet**
  - **Chaque port possède une adresse Ethernet**
- **Matériels**
  - **Chassis ou boitier**
  - **Cartes : 2 ports FO, 8/16/24/32/48/64 ports TP … avec débits 10, 100, 1000 Mb/s, LS, ATM, FDDI …**

Elts interconnexion : routeur (IP)

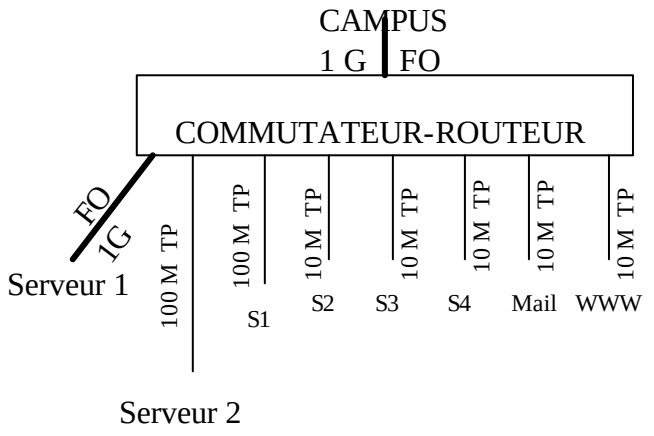
- **Logiciel – performances**
  - **Système d'exploitation**
    - IOS CISCO
  - **Configuration : avec telnet ou navigateur**
  - **Surveillance : SNMP**
  - **Performances :**
    - Nb de paquets routés/s
    - Routage : ASIC
  - **Un PC Linux avec 2 cartes Ethernet peut faire fonction de routeur**
- **Fonctions annexes : chapitre ultérieur du cours**

Elts interconnexion : Commutateur-routeur (IP)

- **Multilayers switch**
- **Réunion des fonctions commutateur et routeur dans une seule « boite »**
- **On peut configurer certains ports en commutation, d'autres en routage**
- **L'équipement à tout faire**
  - **Mais pour le configurer il est nécessaire d'avoir défini l'architecture que l'on veut mettre en place**
- **Maintenant très performant avec des prix très compétitifs**
  - **Remplace les routeurs et les commutateurs**

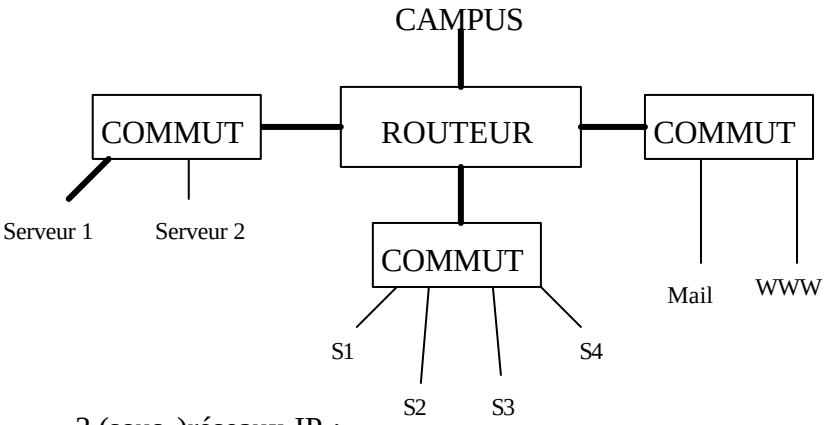
Elts interconnexion : commut-routeur

- **Exemple de réseau de laboratoire**



Elts interconnexion : commut-routeur

- **Peut-être équivalent à :**



3 (sous-)réseaux IP :
Serveur 1, Serveur2 – S1, S2, S3, S4 – Mail, WWW

Elts interconnexion : action /trame

Trame Ethernet contenant un datagramme TCP

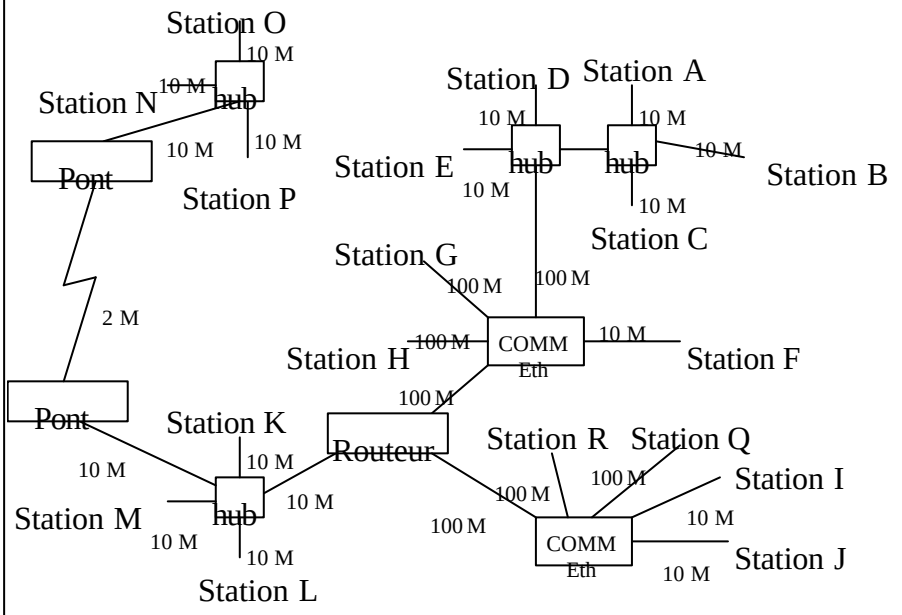
- **Entête Ethernet**
  - **@ Ethernet destination ✍ Pont - Commutateur**
  - **…**
- **Entête IP**
  - **…**
  - **@ IP destination ✍ Routeur**
  - **…**
- **Entête TCP**
  - **…**
  - **Numéro de port destination ✍ Station (choix du service)**
  - **…**
- **Données ✍ Application**

Elts interco : Architecture Eth - IP

Dans une entreprise

- **Entre stations utilisateurs d'un service**
  - **Hubs ou commutateurs**
- **Entre serveurs ou stations demandant du débit (graphiques, …) d'un service**
  - **Commutateurs**
- **Entre services**
  - **Commutateurs ou routeurs**
- **Entre l'entreprise et l'extérieur (Internet)**
  - **Routeurs**

Ex interconnexion de réseaux Ethernet



Ex interconnexion de réseaux Ethernet

- **Trame Eth A ✍ C. Arrive-t-elle à B ? E ? F ?**
- **Trame Eth P ✍ O. Arrive-t-elle à N ? M ?**
- **Trame Eth R ✍ Q. Arrive-t-elle à I ? J ?**
- **Trame Eth A ✍ L. Arrive-t-elle à K ?**
- **A -> Broadcast Eth. Arrive-t-il à B ? D ? G ? R ?**
- **L ✍ Broadcast Eth. Arrive-t-il à K ? O ? D ?**
- **Collision possible entre les 2 trames :**
  - **A ✍ B et D ✍ E ? O ✍ N et M ✍ L ?**
  - **G ✍ H et E ✍ F ?**
- **B a un coupleur défectueux (envoie des trames sans écoute ✍ collisions). Cette station perturbe –t-elle A ? E ? G ? R ?**
- **F dans le même cas. G est-elle perturbée ?**
- **O dans le même cas. M est-elle perturbée ?**

Ex interconnexion de réseaux Ethernet

- **B émet un flot de données de 5 M b/s vers A en continu. Quelle bande passante (théorique) reste-t-il à A ? C ? E ? F ? R ?**
- **G émet un flot de données de 5 M b/s vers H en continu. Quelle bande passante (théorique) reste-t-il à F ? E ?**
- **G émet un flot continu de broadcast à 20 Mbps. Quelle bande passante (théorique) reste-t-il à H ? E ? B ? R ?**
- **O émet un flot de broadcast à 2 Mbps. Quelle bande passante reste-t-il entre N et M ?**
- **Les flots de données en parallèle suivants sont ils possibles ?**
  - **10 Mb/s A-B et 10 Mbps D-E ?**
  - **100 Mb/s R-Q et 10 Mbps I-J ?**
  - **10 Mb/s O-N et 10 Mb/s L-M ?**
  - **10 Mb/s F-G et 10 Mb/s F-H ?**

Liaisons longues distances - opérateurs

- **Liaisons**
  - **Commutées = temporaires ✍ partagées**
    - Pb : phase (+ ou - longue) d'établissement de connexion et de déconnexion ✍ difficile pour un serveur
  - **Permanentes : entre 2 points fixes**
    - LS : Liaisons Spécialisées – Lignes Louées
- **Opérateurs**
  - **Opérateurs Telecom traditionnels : FT, Cegetel, …**
    Mais aussi SNCF, sociétés d'autoroutes, …
  - **Liaisons : FO, câbles cuivre, liaisons hertziennes, …**
  - **Equipements : (dé)multiplexeur, commutateurs (en tous genres), …**
  - **Offres « sur mesure » - contrats spécifiques**
  - **Offres « catalogue » : étudiées ici**
  - **Les services « à valeur ajoutée » (d'interconnexion) seront étudiés dans un chapitre ultérieur**

Liaisons longues distances : utilisations

- **Entreprises :**
  - **Liaisons inter-sites**
  - **Louent des liaisons spécialisées aux opérateurs**
  - **Coût d'installation + coût de location**
- **Particuliers ou petites agences :**
  - **Particulier - domicile ✍ entreprise**
  - **Agence ✍ siège**
  - **Utilisent les réseaux commutés**
  - **Généralement : coût d'installation + location + utilisation**

Liaisons commutées : RTC

Réseau Téléphonique Commuté

- **Equipement : modem V90 56.6 Kb/s (réception)**
  - **Emission à 33.6 Kb/s**
- **Modem micro : interne, externe sur port série …**
- **Particulier/agence ✍ LAN Entreprise**
  - **Micro - Modem – RTC – Serveur d'accès RTC (pool de modems – Concentrateur - Routeur) – LAN (Ethernet) entreprise**
    - Fonction de ré-appel : coût et sécurité
    - Authentification des utilisateurs : protocole – serveur RADIUS
  - **Micro – Modem – RTC – Fournisseur d'accès Internet – Connexion Internet –Routeur – (Garde-barrière) - LAN entreprise**

Liaisons commutées : RTC

- **IP**
  - **Protocole niveau 2**
    SLIP ✍ PPP (Point to Point Protocol)
  - **Micro : @ IP statique ou dynamique (DHCP)**
- **Liaison non permanente**
  - **Le micro ne peut pas être serveur**
- **Toujours très utilisé**
  - **Réseau RTC partout**
  - **Toujours plus de débit possible sur la paire torsadée**

Liaisons commutées : RNIS

Réseau Numérique à Intégration de Service

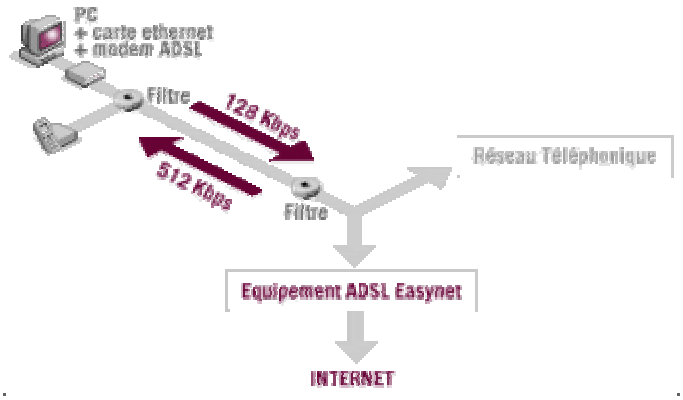
- **ISDN (surtout Europe et Japon)**
- **Réseau national de FT : Numéris**
- **Accès de base (particulier-agence) : 144 Kb/s**
  - **2 canaux B à 64 Kb/s : téléphone + Internet par exemple**
  - **1 canal D à 14 Kb/s : signalisation**
  - **Utilisation liaison téléphonique classique**
  - **25,5 E / mois en oct 02 (Numeris Itoo)**
- **Accès primaire (Entreprise : PABX) : ~ 2 Mb/s**
  - **30 canaux B à 64 Kb/s + 1 canal D à 64 Kb/s**

Liaisons commutées : RNIS

- **Connexion micro (particulier-agence)**
  - **« Modem » RNIS : carte micro ou « modem » externe sur port série**
  - **Modem RTC - Boitier RNIS avec 2 prises téléphoniques**
  - **Chemin : Micro – Modem RNIS – Réseau Numéris – (Modem RNIS) – Serveur d'accès RTC ou PABX - Entreprise**
- **Interconnexion de sites : routeurs RNIS (2B + D)**
- **IP : idem RTC : PPP**
- **L'utilisation n'a jamais vraiment décollé**
  - **Européen, surtout français : pas USA - Cher**
  - **Encore utilisé en back-up ou pour liaisons provisoires**

Liaisons longues distance : ADSL

- **ADSL : Asymmetric Digital Subscriber Line**
- **xDSL : technologie pour transmission à haut débit sur le RTC**



Liaisons longues distances : ADSL

- **Modems :**
  - **512 Kb/s réception - 128 Kb/s émission**
  - **1 M b/s réception – 256 Kb/s émission (ADSL Pro)**
- **La liaison reste libre pour le téléphone**
  - **Bande de fréquences utilisée # fréquences vocales**
  - **Filtres : chez particulier et au répartiteur FT**
- **Contraintes :**
  - **Poste téléphonique < 5 km d'un répartiteur FT**
    - Le cas de 80 % des foyers français
  - **Que le répartiteur FT soit connecté à un réseau ADSL**
  - **Abonnement**
    - ADSL chez FT ou ailleurs
    - Chez un fournisseur accès Internet
    - Pack qui inclut les 2

Liaisons longues distances : ADSL

- **Liaison particulier – entreprise :**
  - **Micro – coupleur Ethernet ou port USB – Modem ADSL – RTC – FAI ADSL – Internet – Routeur – LAN Entreprise**
- **IP : idem Ethernet**
- **Connexion permanente :**
  - **Coût installation et mensuel (pas à la consommation)**
  - **Possibilité de connecter un routeur côté particulier ou agence mais fournisseur d'accès obligatoire**
- **Offre FT :**
  - **Sans Internet : 30 E / mois ou 107 E / mois (ADSL Pro) en oct 02**
- **De plus en plus utilisé**
  - **Pbs : monopole de FT, disponibilité selon le lieu**
  - **Devrait devenir l'accès standard**

Liaisons longues distances : X25

- **Réseau à commutation de paquets :**
  - **Couches 2-3**
  - **Circuits virtuels**
  - **Adresses X25**
- **Opérateur historique : Transpac**
- **Accès jusqu'à 64 Kb/s (ou guère plus)**
- **Les serveurs vidéotex (minitel) ont une connexion X25**
- **Remplacé par IP sous toutes ses formes**

Liaisons spécialisées FT

- **Transfix (nationales)**
  - **2.4 K b/s à 34 Mb/s**
  - **STAS : Spécifications Techniques d'Accès au Service**
  - **2.4 K à 19.2 K : interfaces : V24, V28**
  - **64 K à 34 M : interfaces : X24/V11 ou G703-G704**
  - **Modems fournis par opérateur**
  - **Liaisons internationales : idem nationales mais plus difficiles à mettre en place de bout en bout : sur-mesure**
- **Connexions :**
  - **Routeurs**
  - **Ponts (distants)**
  - **Commutateurs ATM**
  - **PABX Téléphoniques**

Liaisons longues distances : modems

- **MOdulateur DEModulateur**
  - **Convertisseur digital/analogique ou adaptateur digital/digital destiné à transporter des données sur des lignes point à point**
- **Plusieurs types de modems :**
  - **RTC : Liaisons commutées : asynchrones historiquement**
  - **LS : Liaisons permanentes : synchrones**
  - **RNIS**
  - **Câble**
  - **ADSL**
  - **TV**
  - **…**

Modems RTC

- **Programmation :**
  - **Commandes AT (origine Hayes)**
- **Fonctions :**
  - **Contrôle de flux XON/XOFF ou RTS-CTS**
  - **Correction d'erreur (MNP 34, V42, ARQ)**
  - **Compression (MNP5, MNP7, V42Bis)**
  - **Adaptation automatique débits et fonctions**

ATM : plan

- **Objectifs**
- **QoS : Qualité de Service**
- **Couches 1 et 2**
- **Commutateurs**
- **Routage**
- **Architectures LS et LANE**
- **Bilan**
- **Exemple**

ATM : objectifs

- **ATM : Asynchronous Transfert Mode**
- **Origine : CNET (FT R&D)**
  - **Opérateur téléphone à l'origine**
- **Supporter tout type de communication Voix – Vidéo - Données informatiques**
- **Mieux utiliser la bande passante**
  - **Téléphonie longue distance**
- **Fonctionner à très hauts débits : Gbits/s**
- **Garantir une qualité de service (QoS) à chaque utilisateur (application) de bout en bout**
- **Démarche très théorique**

ATM : objectifs

- **Mêmes protocoles et technologies en LAN, MAN et WAN**
- **Caractéristiques des réseaux / services attendus**
  - **Bande passante (bps) partagée : garantie si possible**
  - **Temps de latence (délai de transmission) : minimum et constant si possible**
    - Dépend distance, éléments actifs, charge (files d'attente)
  - **Jitter (variation temps de latence) : min si possible**
  - **Taux de pertes : min si possible**
  - **…**

ATM veut fournir ces services

✍ **Protocoles et technologies complexes**

ATM : Exemple de QoS : Téléphonie

- **Entendre tous les mots**
  - **Faible taux de pertes**
    - Contrainte : bit error rate < 10^{-2}
  - **Débit constant garanti**
    - Contrainte : 64 Kbits/s sans compression ---> 5 Kbits/s avec
- **Recevoir au même rythme que l'émission**
  - **Temps de latence fixe : contrainte : jitter < 400 ms**
- **Dialogue possible**
  - **Temps de latence faible**
  - **Poste avec annulation d'echo**
- **Retransmissions : inutiles**
- **Mode connecté bien adapté**
- **Exemple d'incompatibilité (théorique)**
  Téléphone et Ethernet

ATM QoS : classes de service

- **Problème : pour supporter toutes les qualités de service sur tous les réseaux ATM il faudrait sur-dimensionner :**
  - **Les liaisons : bande passante et caractéristiques**
  - **Les équipements : performances et fonctionnalités**
- **Solution ATM :**
  - **On regroupe les applications qui demandent des qualités de service similaires ✍ 4 groupes**
  - **On définit 4 classes de services que peuvent offrir les réseaux (liens et équipements) ATM qui correspondent aux 4 groupes : UBR, ABR, CBR, VBR**

ATM QoS : classes de services

- **UBR – Unspecified Bit Rate**
  - **Les applications peuvent émettre un flux variable jusqu'à un débit maximum**
  - **Réseau : aucune garantie – pas de contrôle de flux**
  - **Service très dégradé**
- **ABR – Available Bit Rate**
  - **Pour supporter des applications qui peuvent utiliser toute la bande passante disponible, avec un service « Best Effort » de type IP**
  - **Exemples : applications qui utilisent TCP (FTP, HTTP, …), interconnexion d'Ethernets**
  - **Services réseau**
    - Aucune garantie (bande passante, temps de latence, …)
    - Mais mécanisme de contrôle de flux

ATM QoS : classes de services

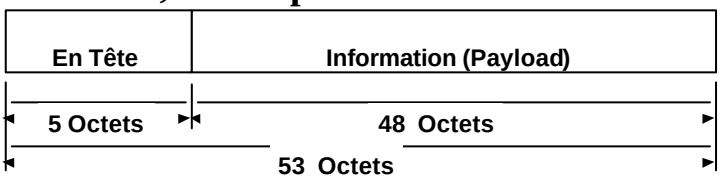
- **CBR – Constant Bit Rate**
  - **Pour supporter les flux à débit constant de données**
  - **Exemple d'application : téléphone**
  - **Services réseau : bande passante réservée, temps de latence fixe**
- **VBR – Variable Bit Rate**
  - **Pour supporter les applications à débit variable mais qui demandent certaines garanties (par exemple une bande passante minimum garantie à tous les instants)**
  - **Exemple : multimédia : vidéo compressée à débit variable …**
  - **Services réseau :**
    - Bande passante minimum garantie
    - Bande passante maximum garantie pendant un temps maximum fixé
    - Temps de latence
    - ….
  - ✍ **Très complexe à réaliser**

ATM 1-2 : mode connecté

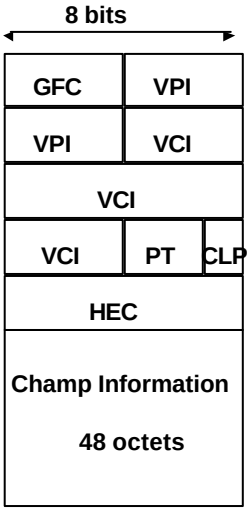
- **Problème : quand demande-t-on une (des) qualité(s) de service au réseau ?**
- **Statiquement : à l'abonnement**
  - **(Ou lors de la conception du réseau)**
- **A chaque session : mode connecté**
  - **Ouverture d'une connexion de bout en bout**
    - En indiquant ce dont on a besoin
  - **Transfert d'informations**
  - **Fermeture d'une connexion**
- **Appel destinataire (ouverture connexion)**
  - **Adresse destinataire ✍ Numéro de VP et de VC**

ATM 1-2 : les cellules

- **Données dans des cellules**
- **Taille fixe : 53 octets**
  - **Compromis**
    - Petite (avantage : faible temps de propagation, …)
    - Grande (avantage : moins de traitements, …)
  - **Facilite les implémentations hardware**
  - **Facilite l'allocation de bande passante**
- **Ni détection, ni récupération d'erreur**



ATM 1-2 : structure de la cellule



GFC Generic Flow Control

VPI Virtual Path Identifier (8 bits : 256)
VCI Virtual Channel Identifier
(16 bits : 64000 possibilités)

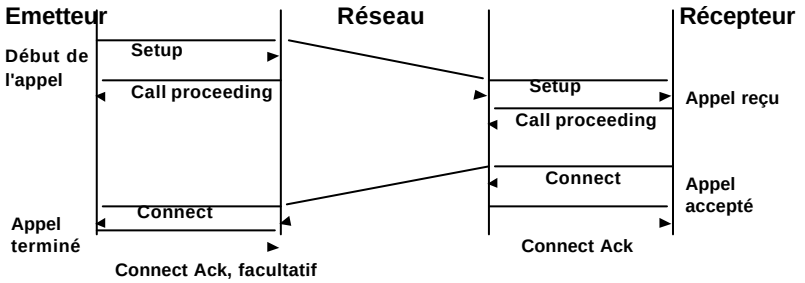
PT Payload Type
Message d'administration ou d'information
Etat de congestion
(MAJ par commutateur)

CLP Cell Loss Priority
"priorité" à la destruction si 1

HEC Header Error Check
sur l'en-tête de la cellule

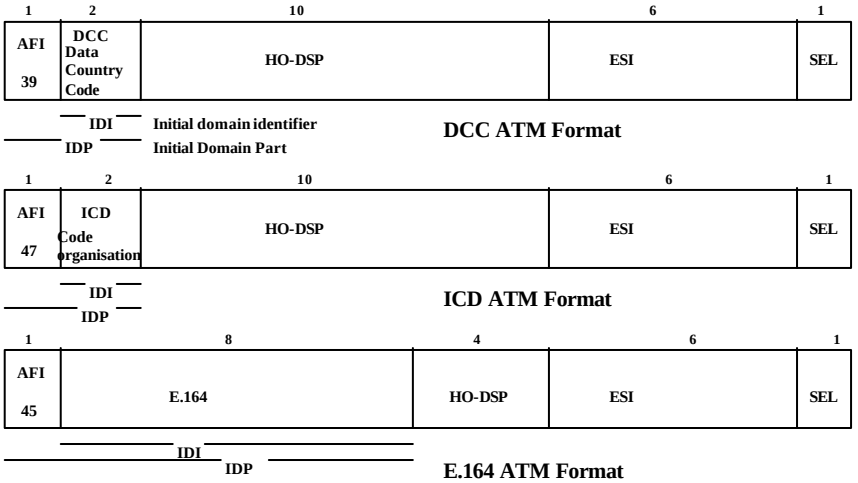
ATM 1-2 : UNI (standard)

- **UNI : User to Network Interface**
  - **Comment établir une connexion**
  - **Comment la rompre**
  - **Format des paramètres de qualité de service**
    - Débit, taux d'erreur, temps de latence, …
  - **Format d'adresse : 20 octets**



Etablissement connexion

ATM 1-2 : adresses : 3 types



AFI : Identificateur de l'autorité et du format

HO-DSP : High Order Domain Specific Part, utilisé pour supporter des protocoles de routages hiérarchiques.

ESI : End System Identifier, en fait la MAC adresse (idem Ethernet)

ATM 1-2 : liaisons

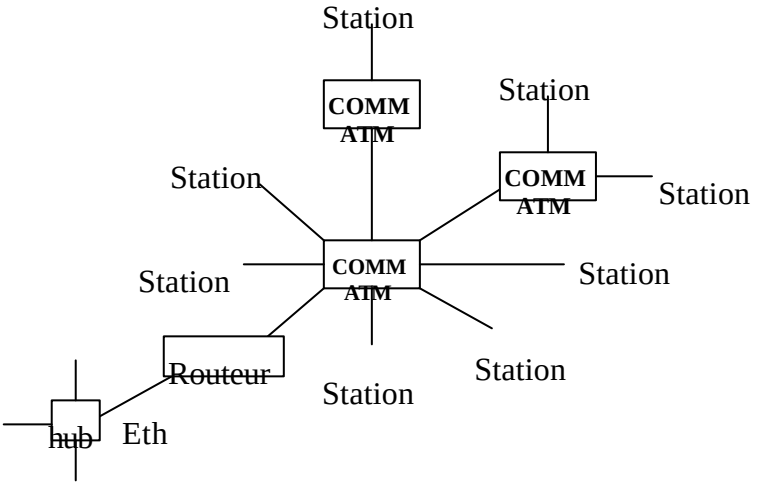
- **Point à point**
- **Liaisons spécialisées câble cuivre (longues distances)**
  - **E1 (2 Mbits/s), E2 (34 Mbits/s)**
  - **T1 (1.5 Mbits/s), T3 (45 Mbits/s)**
  - **….**
- **Liaisons FO**
  - **FO multimode 155 Mbits/s (OC 3)**
  - **FO multimode ou monomode 622 Mbits/s (OC12)**
  - **….**
- **Liaisons TP**
  - **155 Mbps UTP cat5**
  - **52 Mbps UTP cat3**
  - **….**

ATM : commutateurs ATM

- **Eléments d'interconnexion de niveau 2**
- **Commutateur ATM**
  - **Interconnecte des liaisons ATM (point à point)**
  - **Commute les cellules sur une liaison ou une autre / table de routage**
- **Cellule contient les numéros de VP et de VC**
  - **Etablissement des VP et VC**
    - Statiquement
    - Dynamiquement lors de l'ouverture de la connexion

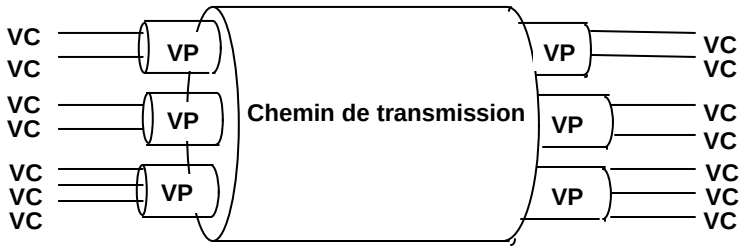
ATM : commutateurs ATM

- **Structure d'un réseau ATM**



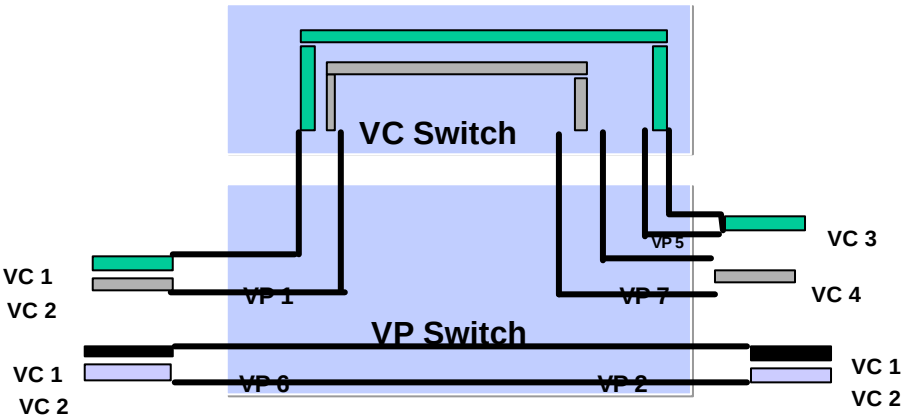
ATM : commutateurs

- **VP et VC**

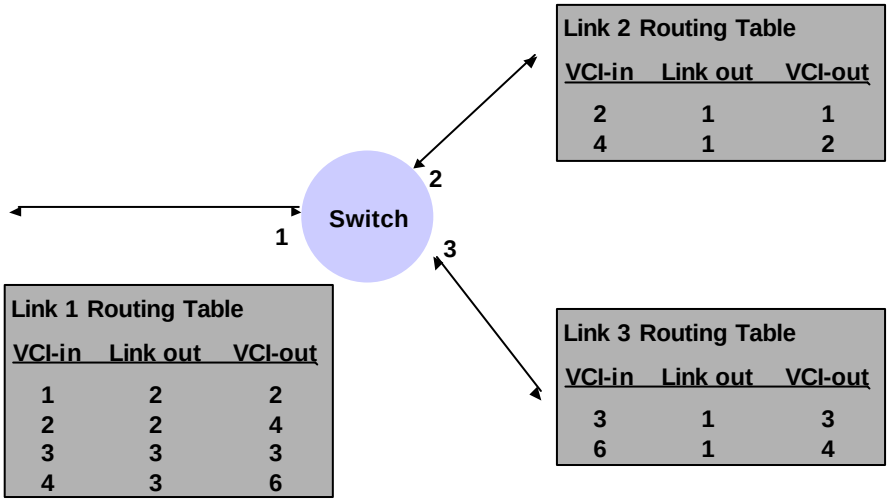


ATM : commutateurs

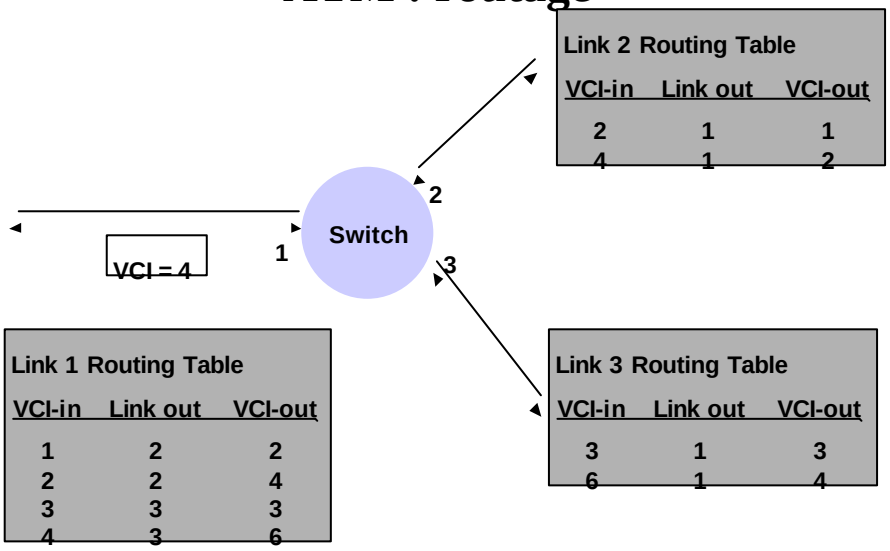
- **Commutateur de VP et de VC**



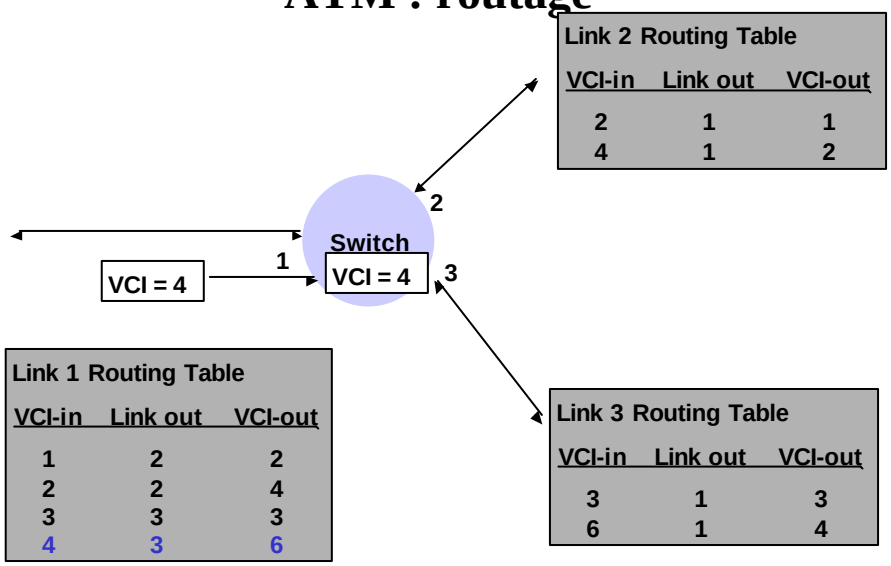
ATM : routage



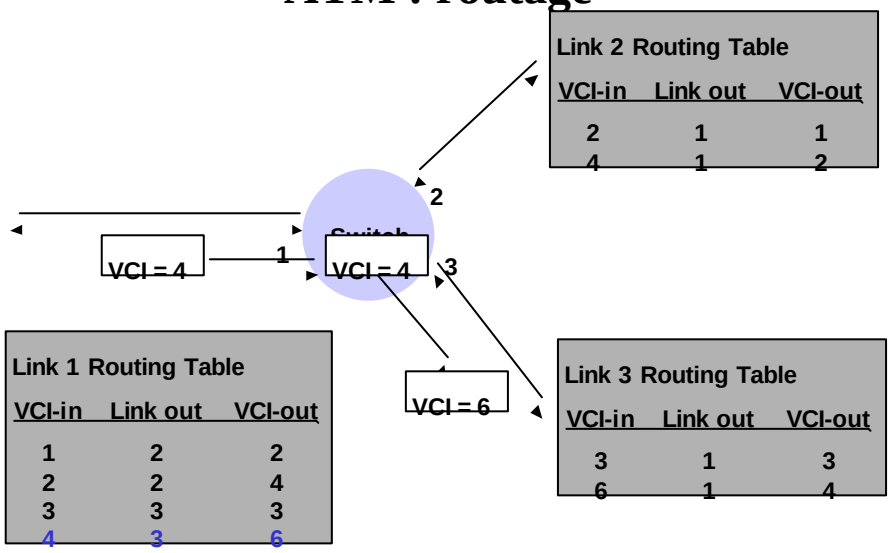
ATM : routage



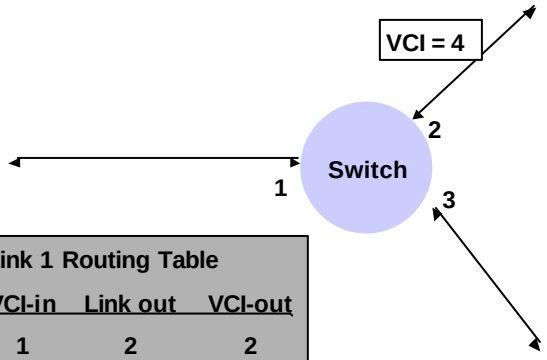
ATM : routage



ATM : routage



ATM : routage



Link 2 Routing Table

VCI-in	Link out	VCI-out
2	1	1
4	1	2

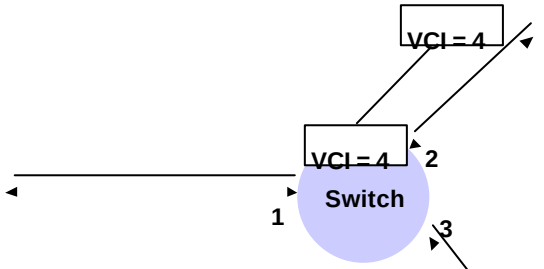
Link 3 Routing Table

VCI-in	Link out	VCI-out
3	1	3
6	1	4

Link 1 Routing Table

VCI-in	Link out	VCI-out
1	2	2
2	2	4
3	3	3
4	3	6

ATM : routage



Link 2 Routing Table

VCI-in	Link out	VCI-out
2	1	1
4	1	2

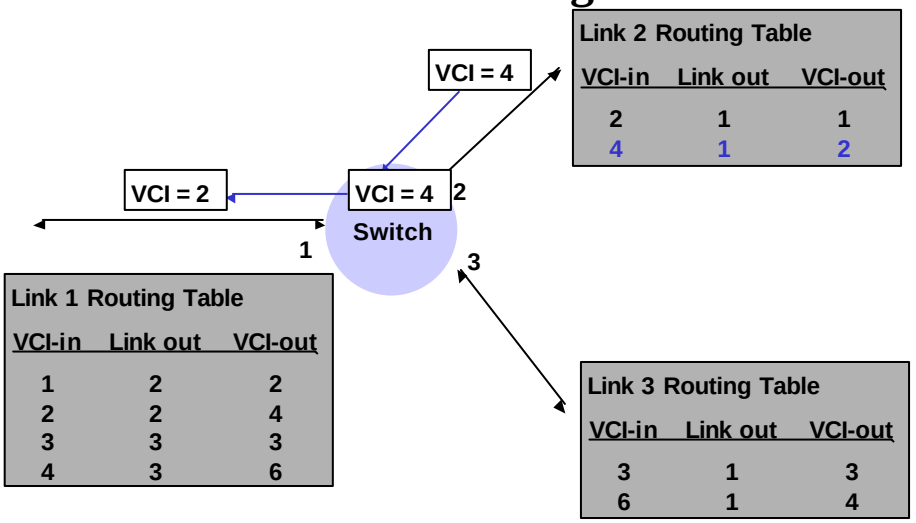
Link 3 Routing Table

VCI-in	Link out	VCI-out
3	1	3
6	1	4

Link 1 Routing Table

VCI-in	Link out	VCI-out
1	2	2
2	2	4
3	3	3
4	3	6

ATM : routage



Link 2 Routing Table

VCI-in	Link out	VCI-out
2	1	1
4	1	2

Link 1 Routing Table

VCI-in	Link out	VCI-out
1	2	2
2	2	4
3	3	3
4	3	6

Link 3 Routing Table

VCI-in	Link out	VCI-out
3	1	3
6	1	4

Tables de routage ATM

Table de routage port 1

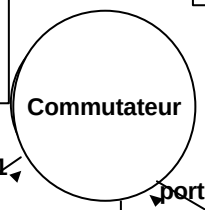
VCI-in	Port- out	VCI-out
2	2	2
3	3	6

Table de routage port 2

VCI-in	Port- out	VCI-out
2	1	2
4	3	8

Table de routage port 3

VCI-in	Port- out	VCI-out
6	1	3
8	2	4



Station A

Table de routage

Station	VCI
B	2
C	3

Station B

Table de routage

Station	VCI
A	2
C	4

Station C

Table de routage

Station	VCI
A	6
B	8

Architectures ATM

- **On peut bâtir plusieurs types d'architecture sur un réseau ATM**
  - **Liaisons spécialisées point à point**
  - **Des réseaux LANE : émulation de LAN**
  - **Des réseaux classical IP : architecture IP**
    - Traité dans la partie « Architecture IP »
- **Et on peut mixer l'ensemble**
  - **Ce que font les opérateurs**

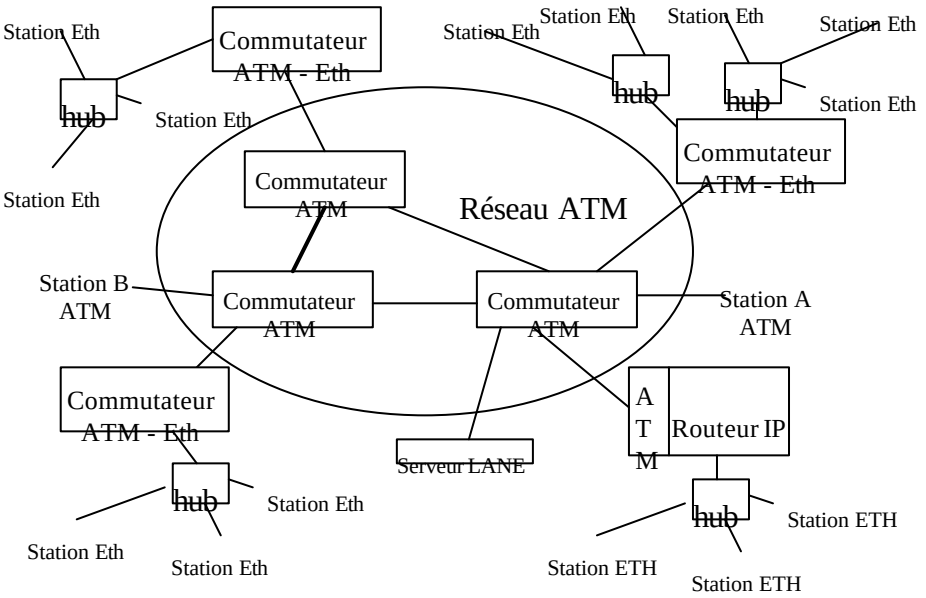
Architecture ATM : Liaison spécialisée

- **Utilisation courante : location de VC ou de VP entre 2 sites à un opérateur qui possède un réseau ATM**
  - **WAN**
  - **Débit demandé pour la liaison**
  - **Certaines qualités de service assurées : ABR, CBR, …**
- **Connexion des sites aux extrémités :**
  - **Commutateur ATM**
    - S'il y a un réseau ATM sur le site, permet de garantir certaines qualités de service jusqu'à l'intérieur du site.
  - **Routeur IP (fourni par le site) avec une carte ATM**
    - Sur le site : réseaux Ethernets par exemple
    - Routeur fourni ou non par l'opérateur
  - **Commutateur ou routeur Ethernet**
    - L'opérateur fournit l'équipement ATM ✍✍ Ethernet
    - ATM est « invisible » pour le site

Architecture ATM : LANE : buts

- **LANE : LAN Emulation**
  - **ELAN : Emulated LAN**
- **Objectifs :**
  - **Interconnexions (niveau 2) de réseaux locaux comme Ethernet à travers un réseau ATM**
  - **Intégration de stations ATM comme « stations Ethernet »**
  - **But : rendre « invisible » les commutateurs ATM aux réseaux Ethernet ✍ LAN emulation**
- **En LAN mais aussi en MAN**

Architecture ATM : LANE : schéma



Architecture ATM : LANE

- **Emule un réseau Ethernet (de commutateurs) :**
  - **Stations Eth + Stations ATM A et B**
  - **Stations ETH ne font pas partie de ce réseau**
- **Sur LANE : interconnexion de niveau 2**
  - **On peut utiliser d'autres protocoles que IP**
- **Logiciels :**
  - **Stations Eth : pas de logiciel spécifique**
    - ATM « transparent »
  - **Stations ATM, routeur IP, Commut ATM-Eth : LEC**
    - LAN Emulation Client
  - **Sur réseau ATM : « serveur » LANE**
    - LECS (Configuration Server)
    - LES (LAN Emulation Server)
    - BUS (Broadcast and Unknown Server)

Architecture LANE : pbs à résoudre

Transformation @ Eth ✍ ✍ @ ATM

- **Lorsqu'une station ATM se connecte sur le réseau**
  (A, B, commutateur ATM-Eth, routeur ATM IP)
  - **Elle connaît l'adresse ATM du Serveur LANE (config manuelle)**
  - **Elle s'enregistre auprès du Serveur LANE :**
    - J'ai telle @ ATM
    - J'ai, ou je connais les @ Ethernet suivantes …
- **Lorsqu'une station ATM veut envoyer une trame Ethernet à une station X**
  - **Interroge le Serveur LANE : qu'elle est l'adresse ATM de la station Ethernet X ?**
  - **Le Serveur lui indique l'adresse ATM**
  - **La station ouvre une connexion ATM avec la station ATM**
  - **….**

Architecture LANE : pbs à résoudre

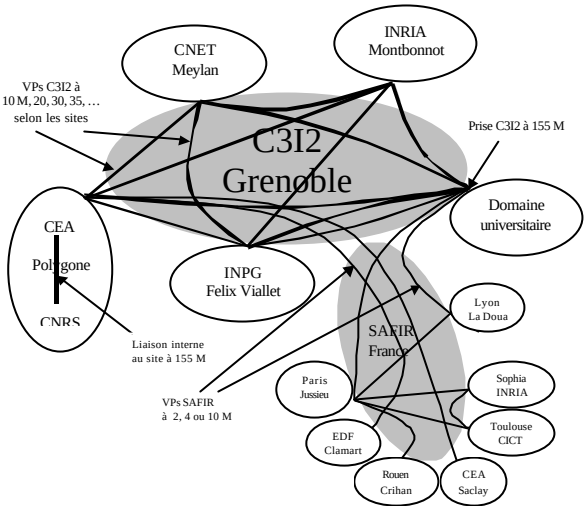
Broadcast Eth ✍ Réseau mode connecté ATM

- **Lorsqu'une station ATM veut envoyer un broadcast Ethernet**
  - **Elle envoie la trame vers le Serveur LANE**
  - **Celui-ci ouvre autant de connexions que de stations ATM sur le LANE**
  - **Il envoie la trame à toutes les stations ATM**
- **Ouverture-fermeture de connexion ATM**
  - **Mécanismes de time-out pour ne pas trop ouvrir ou fermer de connexions ATM**
- **On peut avoir plusieurs ELAN sur un réseau ATM**

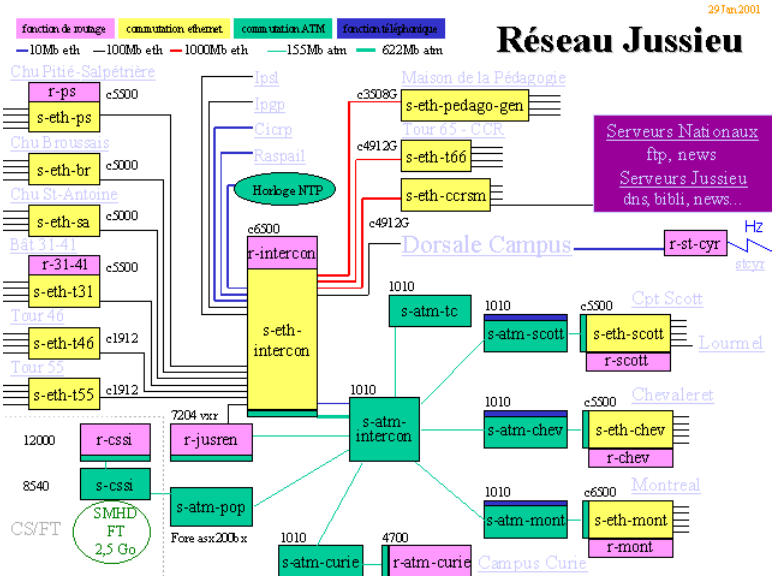
ATM : bilan

- **Très complexe :**
  - **Cher**
  - **Très délicat à faire fonctionner**
- **Utilisé en MAN et WAN par opérateur :**
  - **Location de VC statiques entre 2 points (équivalent de LS)**
    - Reconfiguration lorsque location de nouvelles liaisons
    - Garantit de bande passante
  - **Création de réseaux virtuels ELAN**
- **Utilisation en LAN**
  - **Années 1995-2000**
  - **Remplacé par Gigabit Ethernet maintenant**
  - **Avantage restant : peut intégrer le téléphone (PABX)**
- **Utilisation en MAN et WAN**
  - **Encore très utilisé**
  - **Remplacé par DWDM, IP directement sur FO, …**
- **Bon exemple de réseau multiservices en mode connecté**

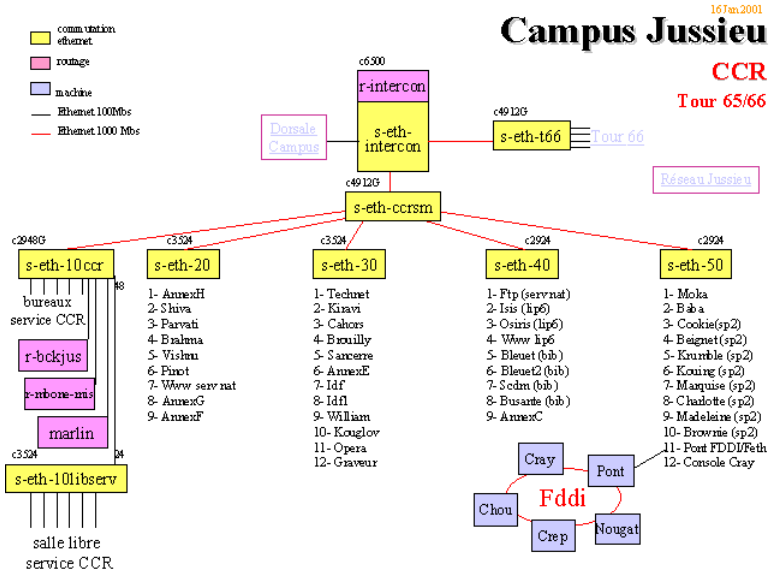
ATM exemple : réseau MAN (C3I2)



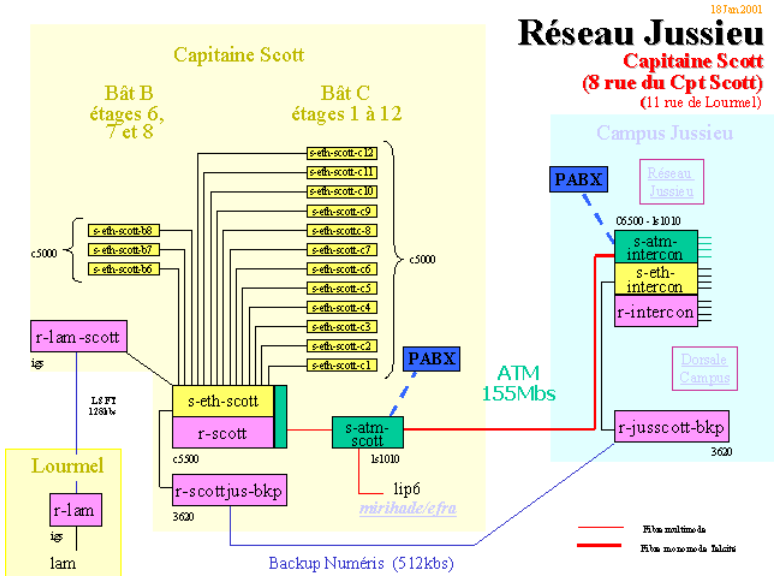
Ex d'architecture : dorsale Jussieu



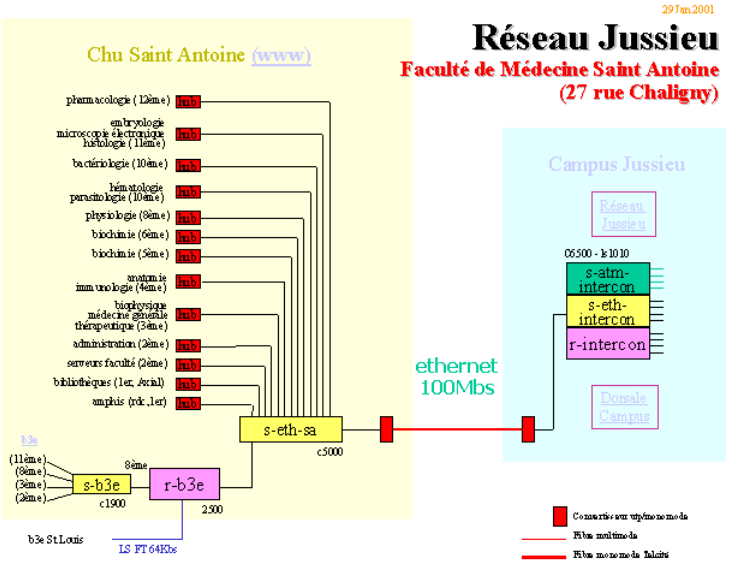
Ex d'architecture : tour



Ex d'archi : interco 2 bâtiments distants



Ex d'archi : interco 2 bâtiments distants



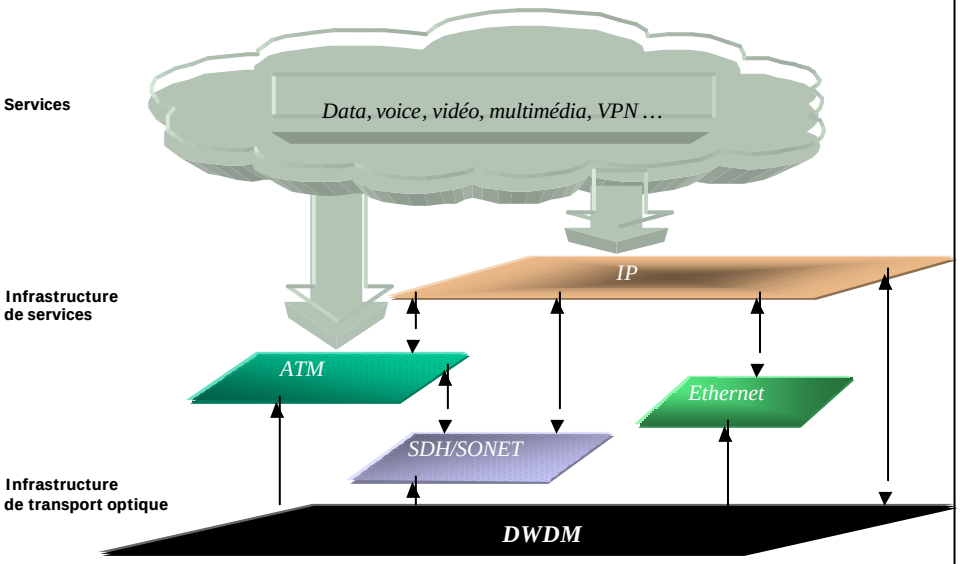
Ex d'archi : RAP : MAN

- **Réseau Académique Parisien**
- **Universités, CNRS, INSERM, …**
  - **300 000 étudiants – 40 000 personnels**
  - **99 sites Paris intra-muros**
- **Réseau privé : ART …**
- **5 POP (Point Of Presence)**
  - **Jussieu (27 sites)**
  - **Odéon (34 sites)**
  - **Auteuil (15 sites)**
  - **Malesherbes (10 sites)**
  - **CNAM (13 sites)**
- **Ouverture: été 2002**

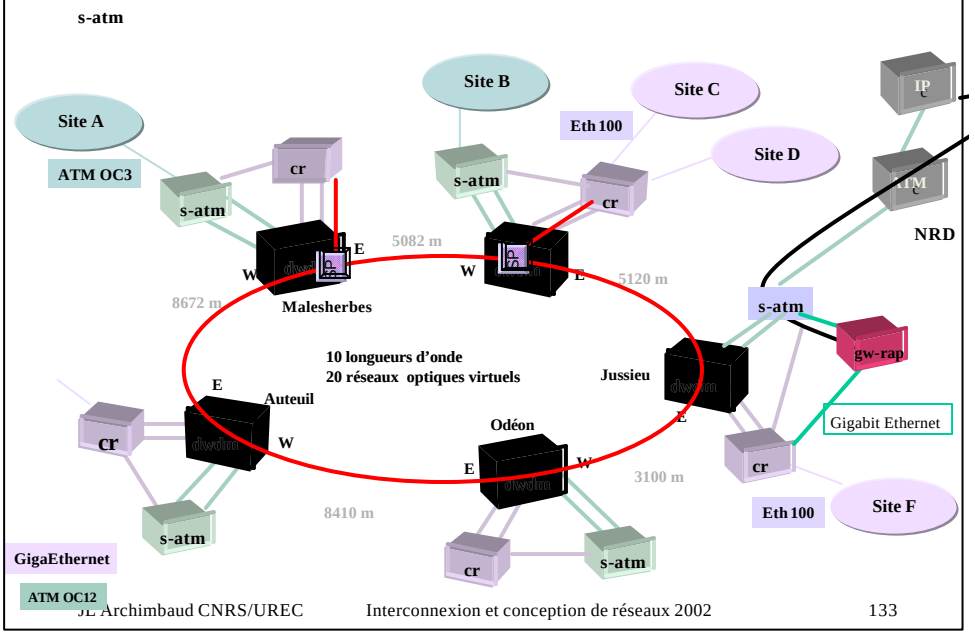
Ex d'archi : RAP : câbles

- **Fibre noire : Single Mode G652**
  - **69 sites**
  - **Lg totale (liaison) : 356.1 km**
  - **Métro : 312 km**
  - **Egouts : 33 km**
  - **Génie civil : 0.3 km**
  - **Plus petite liaison : 1 km, plus grande : 9.6 km**
- **BLR (Boucle locale radio)/ S-HDSL (« ADSL » particulier)**
  - **23 sites à 2 Mbits/s**
- **Faisceaux hertziens**
  - **2 sites proches de Paris**

Ex d'archi : RAP : services réseau



Ex d'archi : RAP : Architecture

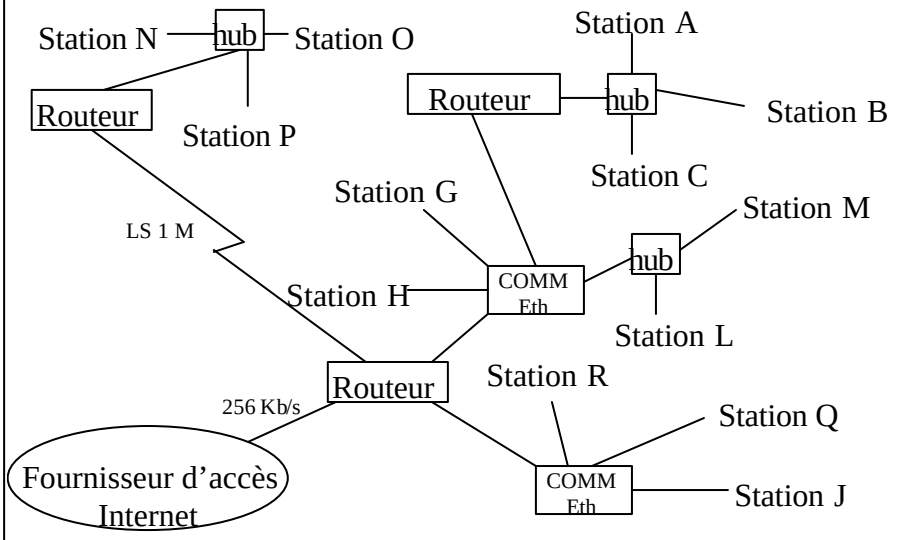


Architecture logique IP : plan

Dans ce chapitre : réseau = réseau IP

- **Adresses IP**
- **Affectation statique ou dynamique (DHCP)**
- **Plan adressage IP**
- **Routage IP**
- **Exemple de répartition d'utilisateurs et de services**
- **Architecture ATM : classical IP**

Architecture IP : réseaux IP



Architecture IP : adresses

- **Une adresse IP par coupleur (machine, routeur)**
- **Format : 4 octets notation décimale A.B.C.D**
  - **Ex : 130.190.5.3 193.32.30.150**
- **Une adresse doit être unique au monde**
  - **Pour l'accès depuis l'Internet**
    - ✍ Surtout pour les serveurs
  - **Pas obligatoire pour les stations clientes Internet**
    - ✍ Intervalles d'adresses locales
- **2 ou 3 parties dans une adresse IP :**
  - **@ de réseau – (@ sous-réseau) - @ machine**
- **Elément qui sépare 2 (ou +) réseaux ou sous-réseaux IP : routeur (ou commut-routeur)**

Archi IP : @ (ancienne classification)

- **Classe A : A.B.C.D avec A ? 127**
  - **1er octet : @ de réseau : 126 réseaux possibles**
  - **Reste : 254 x 254 x 254 (16 M) machines adressables**
  - **Ex : DEC : 16.0.0.0 MIT : 18.0.0.0**
- **Classe B : 128 ? A ? 191**
  - **2 premiers octets : @ de réseau**
    - 64 x 254 : 16 000 réseaux possibles
  - **Reste : 254 x 254 (64 000) machines adressables**
  - **Ex : IMAG : 129.88.0.0 Jussieu : 134.157.0.0**
- **Classe C : 192 ? A ? 223**
  - **3 premiers octets : @ de réseau**
    - 31x 254 x 254 (2 M) de réseaux possibles)
  - **Dernier octet : 254 adresses de machines**
    - IBP : 192.33.181.0 CITI2 : 192.70.89.0

Archi IP : sous-réseaux (subnets)

- **Sous-réseaux : découpage d'un réseau IP (classe A, B, C)**
- **Les sous-réseaux d'un même réseau (subnetté) devaient avoir une taille identique (contrainte routeurs) :**
  - **Masque de subnet spécifiait le découpage**
  - **Bits qui désignent la partie réseau + sous-réseau = 1**
  - **192.33.181.0 découpé en 4 sous-réseaux**
    - Masque 255.255.255.192
    - 192.33.181.0-192.33.181.63
    - 192.33.181.64-192.33.181.127
    - 192.33.181.128-192.33.181.191
    - 192.33.181.192-192.33.181.255
- **Les routeurs permettent maintenant de créer des sous-réseaux de tailles différentes**
- **Les sous-réseaux sont connexes**
  - **Non séparés par un autre réseau IP**
  - **Découpage en sous-réseaux n'est connu que du propriétaire du réseau (site, entreprise, provider, …), pas de l'Internet**

Archi IP : classless

- **Pour obtenir une adresse de réseau (unique)**
  - **Auprès de son fournisseur d'accès à l'Internet**
  - **AFNIC (France) – RIPE (Europe)**
  - **Classe A : impossible**
  - **Classe B : presque impossible (épuisé)**
  - **Classe C ou partie de Classe C : OK**
- **Nouvelle notation et découpage : classless**
  - **Réseau 129.88.0.0 ✍ Réseau 129.88/16**
  - **Réseau 192.33.181.0 ✍ Réseau 192.33.181/24**
  - **Réseaux (sous-réseaux avant)**
    - 192.33.181.0/26 : 192.33.181.0-192.33.181.63
    - 192.33.181.64/26 : 192.33.181.64-192.33.181.127
    - 192.33.181.128/26 : 192.33.181.128-192.33.181.191
    - 192.33.181.192/27 : 192.33.181.192-192.33.181.223
    - 192.33.181.224/27 : 192.33.181.224-192.33.181.255

Archi IP : @ particulières

- **Classe D : 224? A ? 239 : multicast**
  - **224.10.15.3 : ✍ groupe de stations sur l'Internet (n'importe où)**
- **Classe E : 240 ? A ? 254 : utilisation ultérieure**
- **Adresses locales (ne doivent pas sortir sur l'Internet)**
  - **10.0.0.0 à 10.255.255.255 : 10/8**
  - **172.16.0.0 à 172.31.255.255 : 172.16/12**
  - **192.168.0.0 à 192.168.255.255 : 192.168/16**
- **Loopback (soi-même) : 127.0.0.1**
- **0.0.0.0 : quand station ne connaît pas son adresse**
- **130.190.0.0 : le réseau 130.190/16**
- **130.190.255.255 : broadcast**
  - **Toutes les machines du réseau 130.190/16**

Archi IP : Affection @ IP à une station

- **Configuration statique**
  - **Unix : commande ifconfig**
  - **Windows (2000 pro) : panneau de conf – connexion réseau – TCP/IP**
- **Configuration dynamique : DHCP**
  - **Serveur DHCP (Dynamic Host Configuration Protocol) dans un réseau IP avec une plage d'adresses à attribuer**
  - **Station sans adresse IP fait une demande DHCPDISCOVER**
    - @ IP source 0000 @IP dest 255.255.255.255
    - Contient @ Ethernet et nom de la station
  - **Serveur DHCP répond :**
    - Adresse IP - Masque de sous-réseau – informations de routage
    - Adresses DNS – Nom de domaine
    - Durée du bail
  - **Explication simplifiée (plusieurs serveurs DHCP possibles, …)**
  - **Avantage : pas de conf sur stations, portables, économie d'@**
  - **Désavantage : qui est qui ?**

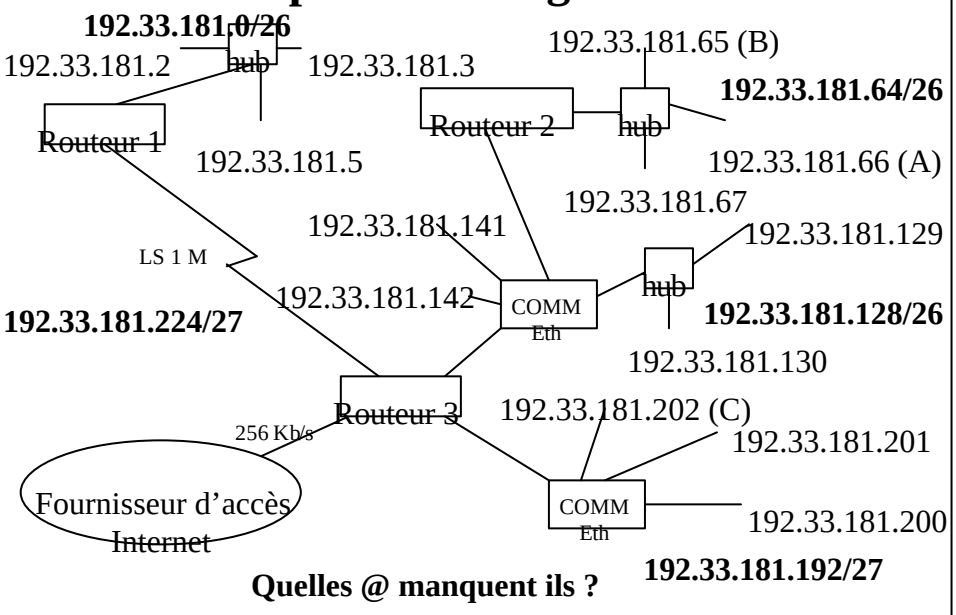
Archi IP : pbs adresses IP

- **Adressage ni hiérarchique, ni géographique**
  - **Tables de routages énormes au cœur de l'Internet**
  - **Distribution des adresses**
    - Au compte-goutte (maintenant bataille commerciale)
- **Uniquement 4 bytes (et certaines plages vides)**
  ✍ **Pénurie d'adresses**
  - **FAI : adresses dynamiques aux clients**
  - **Entreprises – FAI :**
    - Adresses locales sur réseau privé
    - NAT : Network Address Translation
      - Et PAT : Port Address Translation
  - **IPv6**

Archi IP : plan d'adressage

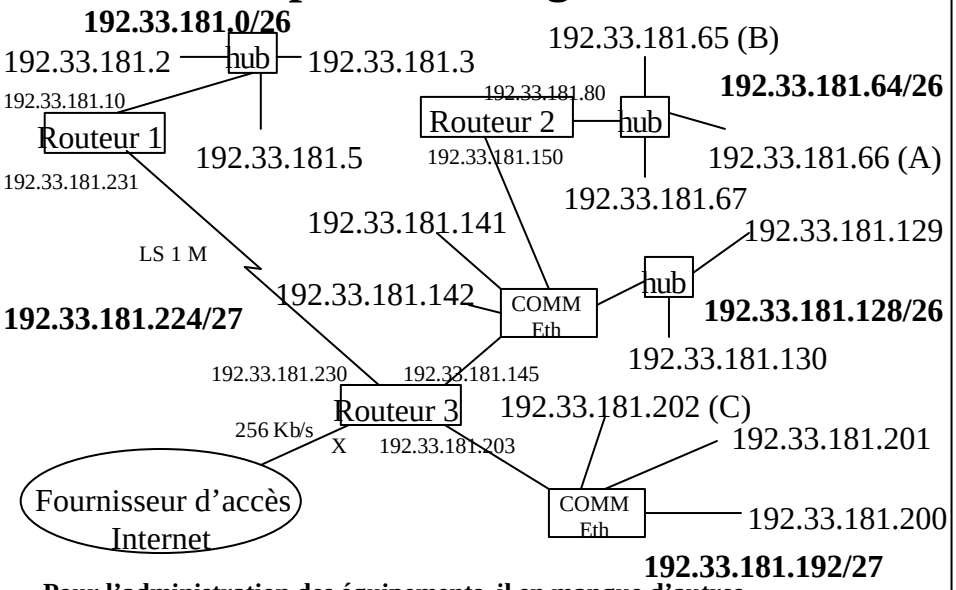
- **Un routeur sépare 2 (ou plus) réseaux ou sous-réseaux IP**
- **Il faut construire un plan d'adressage**
  - **Découper l'espace d'adressage dont on dispose en sous-réseaux et le répartir entre les stations**
- **Eléments à prendre en compte :**
  - **Les routeurs séparent les sous-réseaux**
    - Proximité géographique des stations
    - Ou non si VLAN
  - **Dans un sous-réseau on est dépendant de son voisin**
    - Broadcast Ethernet par exemple
  - **On regroupe dans un même sous-réseau les stations qui travaillent entre elles (d'un service par exemple)**
    - La majorité du trafic reste local au sous-réseau (évite de charger les autres sous-réseaux
    - Profils de connexion et de sécurité identiques

Archi IP : plan adressage 192.33.181/24



Quelles @ manquent ils ?

Archi IP : plan adressage 192.33.181/24



Pour l'administration des équipements, il en manque d'autres …

Archi IP : routage IP

- **A (192.33.181.66) veut envoyer un datagramme IP à B (192.33.181.65)**
  - **Pb : A doit envoyer une trame Ethernet mais ne connaît l'@ Eth B**
  - **Elle envoie un broadcast Ethernet sur le réseau qui demande : quelle est l'@ eth de B ? (l'@ Eth de A est spécifiée dans la trame Ethernet : @ Eth origine)**
  - **B répond à l'@ Eth A en disant : je suis 192.33.181.65 et mon adresse Ethernet est @ Eth B**
  - **A peut alors envoyer alors les datagrammes IP dans des trames Ethernet (elle connaît l'@ Eth de B)**
  - **Mécanisme : ARP – RARP**
- **A (192.33.181.66) veut envoyer un datagramme à C (192.33.181.202)**
  - **Elle doit envoyer une trame Eth au routeur 2 : 192.33.181.80**
  - **Il lui manque cette information ✍ Information de routage**

Archi IP : routage IP

- **Chaque station doit être configurée pour spécifier**
  - **Son adresse IP (Commande Unix ifconfig)**
  - **L'adresse du sous-réseau sur laquelle elle est (Commande Unix ifconfig)**
  - **Une table (de routage) qui indique comment atteindre les autres réseaux (Commande Unix route add)**
- **Exemple A**
  - **@ IP : 192.33.181.66 - @ Réseau : 192.33.181.64/26**
  - **Routes (numéro IP du prochain routeur destinataire) :**
    - 192.33.181.128/26 ✍ 192.33.181.80
    - 192.33.181.224/27 ✍ 192.33.181.80
    - 192.33.181.192/27 ✍ 192.33.181.80
    - 192.33.181.0/26 ✍ 192.33.181.80
    - Reste du monde (default route) ✍ 192.33.181.80
    - La route par défaut (default route - default gateway) suffit
- **Toutes les stations doivent être configurées**
  - **Ex : mon PC dans panneau de configuration …**

Archi IP : routage IP

- **Les routeurs aussi doivent être configurés**
  - **Par port : @ IP, @ Réseau (ou sous-réseau)**
  - **Table routage**
- **Exemple routeur 3 :**
  - **Port 1 : 192.33.181.230 - réseau 192.33.181.224/27**
  - **Port 2 : 192.33.181.145 – réseau 192.33.181.128/26**
  - **Port 3 : 192.33.181.203 – réseau 192.33.181.192/27**
  - **Port 4 : X – réseau Y**
  - **Table routage**
    - Route 192.33.181.64/26 ✍ Port 2 : 192.33.181.150
    - Route 192.33.181.0/26 ✍ Port 1 : 192.33.181.231
    - Route default ✍ Port 4 : routeur du fournisseur d'accès
- **Exemple : envoi datagramme B ✍ C**

Archi IP : routage IP

- **Routage statique**
  - **Mise à jour tables de routage : manuelle**
  - **ICMP redirect : Ce n'est pas ici c'est ailleurs**
  - **Problème : intervention manuelle**
    - Quand le réseau évolue : modification manuel des tables
    - Quand plusieurs chemins possibles et coupures
  - **Utilisé généralement au niveau des stations, dans certains routeurs d'extrémités**
- **Routage dynamique**
  - **Protocoles entre routeurs et entre routeurs et stations pour mettre à jour automatiquement les tables de routages : annonces de routes**
  - **Ex : RIP, OSPF, BGP**
  - **Cf cours sur le routage**

Archi IP : routage IP

- **L'Internet ne fonctionnerait pas sans bons protocoles de routage et sans experts pour les faire fonctionner**
- **C'est une problématique surtout d'opérateurs Internet**
  - **A laquelle s'ajoutent les accords de peering**
- **Routeurs doivent être très rapides**
  - **Traitement du routage directement en ASIC**
- **Routeurs au cœur de l'Internet : doivent connaître toutes routes : impossible ✍ Agrégation de plages d'adresses de réseaux IP**
- **On n'est pas obligé d'avoir une route par défaut sur tous les équipements : sécurité**

Archi IP : répartition d'utilisateurs

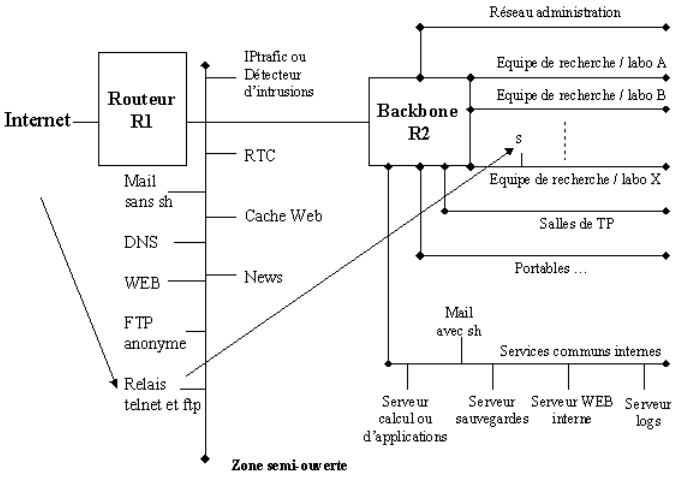
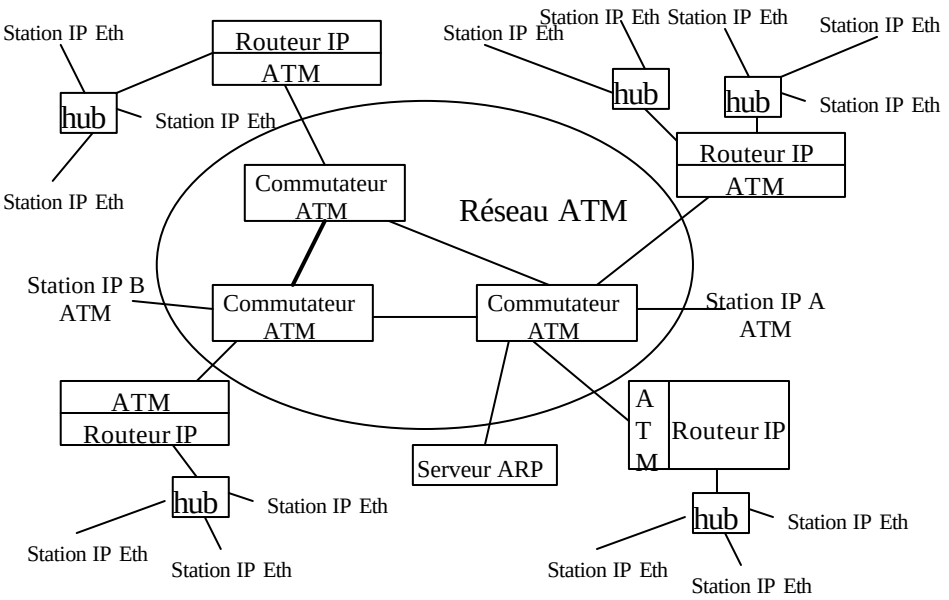


Fig 2 : architecture détaillée

Architecture ATM : classical IP

- **Objectif :**
  - **Utiliser un réseau ATM pour transporter des datagrammes IP**
- **RFC 1483**
  - **Comment encapsuler (transporter) les datagrammes IP dans des cellules ATM**
- **RFC 1577**
  - **Comment construire un réseau IP sur un réseau ATM**
  - **Pb ARP par exemple**

Architecture ATM : classical IP



Architecture ATM : classical IP

- **Un sous-réseau IP dans un réseau ATM**
  - **Un serveur ARP**
  - **Gère une table @ IP ✍✍ @ ATM**
- **Lorsqu'une station ATM IP se connecte**
  - **Elle connaît l'@ ATM du serveur ARP**
    - Configuration manuelle
  - **Elle s'enregistre auprès du serveur ARP**
    - Indique son adresse ATM et son adresse IP
- **Lorsqu'une station ATM-IP veut émettre un datagramme IP vers une autre station ATM-IP**
  - **Demande au ARP Serveur l'@ ATM de la station IP**
  - **Ouvre un VC avec cette station ATM**
  - **…**

Architecture ATM : classical IP

- **Lacunes :**
  - **Pas de broadcast ou multicast IP**
  - **Un seul serveur ARP : pas de redondance : pb si panne**
- **On peut avoir plusieurs sous-réseaux IP sur un réseau ATM :**
  - **Passe par un routeur ATM-IP pour communiquer**
- **ATM complexe avec IP :**
  - **Mode non connecté (IP) avec techno en mode connecté (ATM)**
- **Rq : sur un même réseau ATM on peut avoir :**
  - **Des VC ou VP permanents (ouverts en permanence) :**
    - LS informatique : interconnexions LANs
    - Interconnexions PABX
  - **Des ELAN (plusieurs LANE)**
  - **Des sous-réseaux IP**

MPLS : buts

- **MPLS : Multi Protocol Label Switching**
- **Protocole pour opérateurs de WAN IP**
- **Lacunes d'un réseau WAN IP « classique »**
  - **Travail d'un routeur important**
    - Il doit étudier chaque datagramme
    - Il doit extraire l'@ IP destinatrice du datagramme IP, consulter sa table de routage et agir en conséquence
  - **Pas de partage de charge entre plusieurs liaisons**
    - Il n'y a qu'une route par destination
  - **Pas de routage qui tiendrait compte de qualités de service demandées**

MPLS

- **Les routeurs en bordure de réseau ajoutent (et enlèvent) une étiquette aux datagrammes selon :**
  - **La route que devra emprunter le datagramme**
  - **La classification du datagramme**
    - Prioritaire ou non, pour application avec QoS, …
- **Les routeurs au cœur du réseau routent selon cette étiquette**
  - **Rapide (plutôt de la commutation que du routage)**
- **Protocole pour mettre à jour les tables de routage des routeurs au cœur du réseau :**
  - **Une fois par « flot »**
  - **Choix de route / étiquette donc / origine, QoS, …**
  - **Réservation de bande passante possible**

Intégration téléphonie – informatique

- **Intégration voix - données**
- **Intégration possible car :**
  - **Téléphone et informatique utilisent :**
    - Mêmes câbles (FO, TP) et ondes (hertziennes ou radio)
    - Eléments actifs similaires : les téléphones sont maintenant numériques
  - **Ordinateurs :**
    - Equipés de microphone et hauts-parleurs
    - Pourraient remplacer les postes téléphoniques : poste « unique »
- **Pourquoi intégrer ? : faire des économies**
  - **En réseau d'entreprise**
    - Infrastructure et matériel : même réseau (plusieurs sens à réseau)
    - Même équipe d'administration
  - **Dans les réseaux des opérateurs : mêmes économies**
  - **Au niveau des utilisateurs : économies sur les communications téléphoniques longues distances**
    - Le coût d'une communication téléphonique dépend de la distance
    - Le coût d'une « communication » Internet est indépendante de la distance

Intégration voix-données

- **Pourquoi intégrer ? : apporter des nouveaux services**
  - **Evolution des services informatiques**
    - Chat, mail ✍ mode de communication vocal (téléphonique)
  - **Evolution des services téléphoniques**
    - Communication téléphonique ✍ transfert de documents, vidéo, …
  - **Intégration des services**
    - Annuaires : « téléphoniques » et informatiques (LDAP)
    - Messageries : vocales et électroniques
- **Comment intégrer ?**
  - **Normes existent : H323, SIP**
  - **Solutions techniques (matériels) existent**
  - **Législation s'assouplit : dérégulation du téléphone**
  - **Différents niveaux d'intégration : tranchées ✍ réseau et services**
- **Rappel : contraintes téléphone :**
  - **QoS (voir chapitre ATM précédent) difficiles sur réseau IP**
  - **Existant qui fonctionne parfaitement : PABX à faire évoluer**

Voix-Données : niveaux d'intégration

- **Mêmes tranchées, fourreaux, goulottes … (chemins de câbles) sur un site**
  2 câblages (et équipements actifs) différents
  - **2 réseaux physiques donc logiques différents**
  - **2 administrations différentes**
  - **Fait depuis plusieurs années entre les bâtiments**
  - **Maintenant en pré-câblage de bâtiment**
    - Câblage courants faibles
- **LS longue distance partagée entre 2 sites**
  - **Interconnexion de PABX**
  - **Interconnexion de LAN (routeurs, commutateurs, ponts)**
  - **Ex : LS 2 Mb/s (MIC) ou hertzienne ou laser éclatée (multiplexeur et dé-multiplexeur)**
    - 1 M (16 voix téléphoniques) pour PABX
    - 1 Mb/s pour interconnexion de LAN

Voix-Données : niveaux d'intégration

- **Partage d'un réseau ATM**
  - **VP pour PABX**
  - **VP pour informatique (routeurs, commutateurs)**
  - **FT et les autres opérateurs le font**
- **Utilisation du réseau téléphonique pour les données**
  - **Externe (RTC national) ou interne à l'entreprise**
  - **Ordinateur (ou routeur) – Modem – Réseau téléphonique – Modem – Ordinateur (ou concentrateur ou routeur ou …)**
  - **V90 (56.6 Kb/s), RNIS (2x64 Kb/s), ADSL (… 1 Mb/s)**
- **Utilisation du réseau IP pour la voix**
  - **Téléphonie sur IP**

Voix-Données : Tél / IP : services rendus

- **Connexion ordinateur – ordinateur (application voix)**
  - **Ordinateur – Réseau IP (Eth, PPP) – Ordinateur**
  - **Netmeeting par exemple**
  - **Un réseau logique différent du réseau téléphonique**
    - Pas de communication possible avec postes téléphoniques classiques
  - **Intéressant pour longues distances**
    - Economies en coût de communication
- **Connexion PABX – PABX**
  - **Téléphones – PABX – passerelle – Réseau IP (Eth, ATM, PPP) – passerelle – PABX – Téléphones**
  - **Pas de communication téléphonique possible avec ordinateur connecté dans le mode précédent**
  - **Intéressant si bonne infrastructure IP (beaucoup de débit)**
- **Intégration totale : « le tout IP »**
  - **Communications postes téléphoniques - ordinateurs possibles**

Voix-Données : Tél / IP : H323

- **Origine : monde des téléphonistes ITU**
- **Ensemble complet de standards**
  - **Architecture et fonctions d'un système de vidéo-conférence**
  - **Sur réseaux en mode paquet (sans connexion), sans garantie de QoS comme IP (mais pas uniquement pour IP)**
- **IP : RTP**
  - **Real-time Transport Protocol**
  - **Transport flux temps réel : vidéo, audio, … dans UDP**
  - **Ajoute des informations pour que le récepteur compense : variation latence, arrivée de datagrammes dans le désordre, …**
    - Type de données transportées
    - Horodatage
    - Numéro de séquence

Voix-Données : Tél / IP : H323

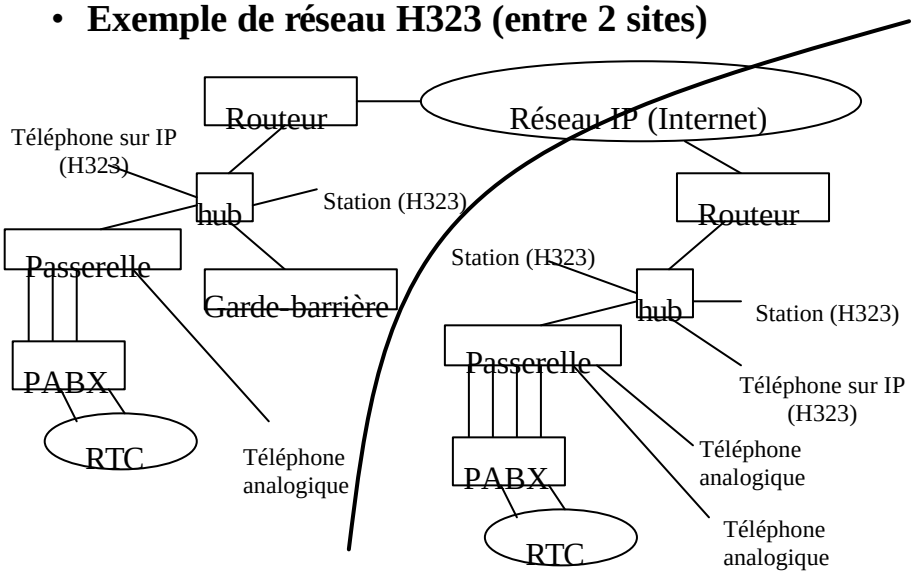
- **IP : RTCP**
  - **Real-time Transport Control Protocol**
  - **Permet d'avertir l'émetteur de la qualité de la transmission :**
    - Le taux de paquets perdus
    - La variation de la latence
    - …
  - **Informations sur l'identité des participants (applications multicast)**
- **Eléments (matériels ou logiciels)**
  - **Terminal H323 :**
    - Ordinateur avec netmeeting
    - Téléphone sur IP (H323)
    - …

Voix-Données : Tél / IP : H323

- **Eléments (matériels ou logiciels) suite**
  - **Passerelle : entre réseau IP et RTC (ou RNIS)**
    - Interfaces :
      - Ethernet ✍ réseau IP
      - Ports TP ✍ téléphones classiques ou PABX
    - Codage/décodage voix, mise en paquets, suppression d'écho, …
  - **Garde-barrière : administration**
    - Gestion des @adresses : IP ✍✍ E164 (téléphoniques)
    - Contrôle les accès
    - Peut refuser des appels si bande passante insuffisante
    - Contrôle une zone (H323)
  - **MCU-Pont : Multicast Control Unit : téléconférence**
    - Gère Multicast
      - Transmet avec adresse IP multicast si le réseau le permet
    - Ouvre n « connexions » point à point

Voix-Données : Tél / IP : H323

- **Exemple de réseau H323 (entre 2 sites)**



Voix-Données : Tél / IP : SIP

- **SIP : Session Invitation Protocol**
- **Origine : IETF : Informatique**
- **Gestion de sessions multimedia avec 1 ou n participants**
- **Adresses : sip:bob@193.10.3.1**
- **Utilise RTP au-dessus de UDP ou TCP**
- **Station IP ✍✍ Station IP : le protocole définit**
  - **Appel – Négociation des paramètres**
  - **Communication**
  - **Fermeture de connexion**

Voix-Données : Tél / IP : SIP

- **Autres services**
  - **Location server (registrar)**
    - Pour qu'un client puisse s'enregistrer quand il change d'adresse IP (mobile, ISP avec adresse dynamique par exemple)
  - **Proxy server**
    - Serveur d'un côté (reçoit les appels)
    - Client de l'autre (émet des appels)
    - Pourquoi ? : Point de contrôle, de facturation
  - **Redirect server**
    - Reçoit des appels
    - Indique la bonne destination à laquelle s'adresser : proxy, …
    - Peut permettre de gérer la répartition de charge entre plusieurs serveurs
- **SIP beaucoup plus basique que H323**

Voix-Données : bilan aujourd'hui

- **Constat : la téléphonie ce n'est pas simple**
  - **Besoin de QoS et habitude de bonne qualité**
  - **Fonctionnalités des PABX et postes téléphoniques sont maintenant complexes : numéros abrégés, transfert d'appel, téléconférence, messagerie vocale, …**
  - **2 équipes d'exploitation avec des cultures différentes**
    - Téléphonistes - informaticiens
- ✍ **Intégration prudente**
  - **Années 1999-2000 : on va tout mettre sur IP**
  - **Aujourd'hui : on peut basculer certaines parties**
- **Elt nouveau : arrivée massive du téléphone portable**
  - **Habitude de communications de moins bonne qualité**
    - Comme le transport de la voix sur un réseau « Best Effort » IP
  - **Portabilité sans comparaison avec ordinateur portable**
    - Ne va pas dans le sens d'un terminal unique : téléphone-ordinateur

Voix-Données : bilan aujourd'hui

- **Dans entreprise :**
  - **Dépend de l'historique et de la culture**
  - **Intégration des 2 équipes d'exploitation ?**
- **Généralement :**
  - **L'utilisateur conserve 2 équipements : téléphone et ordinateur**
  - **Les infrastructures réseaux d'extrémité (câblage horizontal) sont différentes mais chemins identiques**
    - Poste téléphonique : câblage téléphonique ✍ PABX
    - Ordinateur : câblage informatique ✍ hubs, commutateurs, …
  - **Interconnexion de PABX sur IP : solution de + en + déployée**
    - Car débits du réseau données >> réseau téléphonique
    - Avec back-up RNIS par exemple

Voix - Video : n participants

- **N vers n : réunions avec participants distants :**
  - **Téléconférence (voix uniquement)**
    - Service FT (équivalent d'un MCU)
    - Poste téléphonique habituel ou matériel dédié
  - **Matériel de visio-conférence (voix + image)**
    - H323 sur RNIS ✍ H323 sur IP
    - Matériel dédié
    - Netmeeting + Webcam
  - **Multicast IP :**
    - V IC-RAT + Webcam
    - Réseau multicast
    - Académique surtout
- **1 vers n : Visio-conférence (sans question de la salle)**
  - **Idem ci-dessus**
  - **Streaming : realplayer**
    - Unicast ou multicast IP

Réseaux virtuels : plan

- **Pourquoi ?**
- **VLAN : Virtual LAN**
- **Avec ATM**
- **VPN : Virtual Private Network**
  - **PPTP**
  - **L2TP**
  - **IPSEC**

Réseaux virtuels : pourquoi ?

On regroupe dans un même réseau (Ethernet commuté ou IP) les stations qui travaillent ensemble (groupe de travail - workgroup). Conséquences :

- **Les applications « groupe de travail » :**
  - **Qui ont besoin de découvrir les serveurs (contrôleur de domaine, voisinage réseau, imprimantes, serveur DHCP, zone Mac, …)**
  - **Et ces serveurs qui ont besoin d'émettre des messages vers toutes les stations du groupe de travail**

  Utilisent les broadcasts Ethernet ou IP
- **Le groupe qui a les mêmes besoins de sécurité :**
  - **Contrôle l'accès entrant sur le réseau à la frontière du réseau (routeur d'accès)**
  - **Est assuré de la confidentialité par rapport à l'extérieur du groupe car il n'y a pas diffusion à l'extérieur du réseau**

Réseaux virtuels : pourquoi ?

- **Le groupe qui à les mêmes besoins de connectivité depuis et vers l'extérieur :**
  - **Effectue un contrôle d'accès sortant à la frontière du réseau (sur le routeur d'accès)**
  - **Peut mettre en place une limitation de la bande passante utilisée vers l'extérieur au point de sortie**
- **Le groupe peut avoir le même adressage IP et des noms de stations dans le même domaine :**
  - **Réalisé de fait dans un réseau IP**
- **Problème : comment peut on avoir les mêmes services avec un groupe géographiquement dispersé ?**
- **Solution : avec des réseaux virtuels**

Réseaux virtuels : pourquoi ?

- **Exemples de groupes dispersés**
  - **Université UJF sur plusieurs sites à Grenoble et un à Valence**
    - Besoin de regrouper les sites dans un seul réseau logique
  - **Entreprise multi sites interconnectés par Internet :**
    - Même besoin
  - **Formation d'ingénieurs sur 2 sites ENSIMAG-ENSERG**
    - Même besoin
  - **Unité CNRS (UREC) sur 4 villes**
    - Même besoin
- **Exemples de services dispersés**
  - **Services administratifs (DR) du CNRS**
  - **Services comptabilité d'une entreprise multi-sites**
- **Mais aussi des groupes mobiles**
  - **Ordinateurs mobiles**
  - **Déménagements, réorganisations ✍ éclatements géographiques des équipes**

Réseaux virtuels : principes

- **Regrouper « logiquement » un groupe de stations dispersées géographiquement**
  - **Dans un même réseau : Ethernet ou IP ou …**
- **Buts :**
  - **Utilisation d'applications « groupe de travail »**
  - **Sécurité**
  - **Contrôle de bande passante**
  - **Noms et adresses IP**
  - **Mobilité**
- **Plusieurs techniques suivant les buts, WAN/LAN, …**
  - **VLAN**
  - **ELAN**
  - **VPN**

Réseaux virtuels : VLAN

- **Virtual LAN**
- **But : créer un réseau virtuel de niveau 2**
  - **Un domaine de broadcast (Ethernet)**
- **Possible avec des commutateurs Ethernet**
  - **Pas avec des hubs**
  - **Intelligence dans les commutateurs (et routeurs)**
- **Différents types de VLANs**
  - **Par ports (de commutateur) : niveau 1**
  - **Par adresse MAC (Ethernet) : niveau 2**
  - **Suivant la valeur d'autres champs : niveau 3**
    - Protocole, @ IP, …

Réseaux virtuels : VLAN par ports

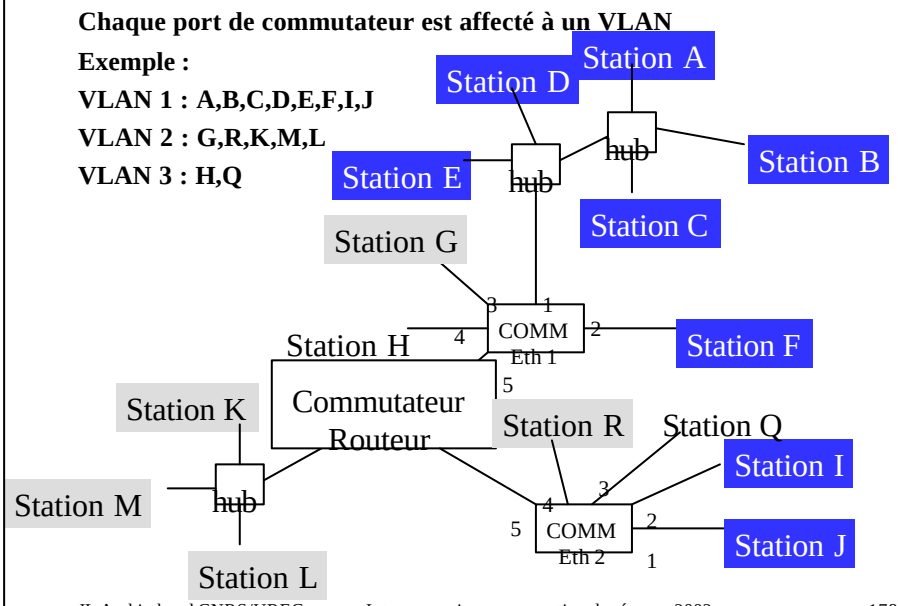
Chaque port de commutateur est affecté à un VLAN

Exemple :

VLAN 1 : A,B,C,D,E,F,I,J

VLAN 2 : G,R,K,M,L

VLAN 3 : H,Q



Réseaux virtuels : VLAN par ports

- **Configuration VLAN de Eth 1 : 3 VLANS 1-2-3**
  - **Port 1 = VLAN 1** **Port 4 = VLAN 3**
  - **Port 2 = VLAN 1** **Port 3 = VLAN 2**
  - **Port 5 = Voir après**
  - **Quand Eth1 reçoit une trame de A (VLAN 1) :**
    - Envoie vers port 2 (et port 5 : cf après)
- **Configuration VLAN de Eth 2 : 3 VLANS 1-2- »**
  - **Port 1 = VLAN 1** **Port 3 = VLAN 3**
  - **Port 2 = VLAN 1** **Port 4 = VLAN 2**
  - **Port 5 = Voir après**
  - **Quand Eth1 reçoit une trame de I (VLAN 1) :**
    - Envoie vers port 1 (et port 5, cf après)
- **Configuration commutateur de Eth1 (idem Eth2) :**
  - **Port 1 : @ MAC A, B, C, D, E**
  - **…**

Réseaux virtuels : VLAN par port

- **Diffusion**
  - **Les équipements Eth1, Eth2 et le commutateur-routeur font en sorte que :**
    - Quand A envoie un broadcast Ethernet ✍ A,B,C,D,E,F,I,J (VLAN1)
      mais pas vers les autres stations
- **Pour communiquer entre Eth1, Eth2, Eth3**
  - **Trame Ethernet F ✍ G impossible**
    - Datagramme IP : F ✍ Commutateur-routeur ✍ G
  - **Passe par routeur ou commutateur-routeur**
- **Remarque**
  - **Cette segmentation peut aussi être réalisée par brassage manuel dans le local technique où sont les commutateurs : dans certains cas**

Réseaux virtuels : VLAN 802.1Q

- **Problème : numéro de VLAN sur les truncks**
  - **Schéma précédent : lorsque le commutateur Eth 2 reçoit une trame Ethernet venant de A, pour savoir vers quelles stations il doit la rediffuser il faut qu'il sache le numéro de VLAN dont A est membre**
  - ✍ **Il faut qu'il trouve cette information dans la trame**
- **Il faut que sur chaque lien entre les commutateurs (truncks) les trames soient marquées (taggées)**
  - **Protocoles propriétaires : ISL (CISCO)**
  - **IEEE802.1Q**
    - Champ type Eth : 8100
    - Champ numéro de VLAN : 12 bits (4096)
    - Niveau de priorité : 3 bits ✍ QoS
    - ….
    - Informations de la trame initiale
- **Schéma précédent : 802.1Q est activé entre Eth 1 – Commut-Routeur – Eth 2**

Réseaux virtuels : VLAN par @ MAC

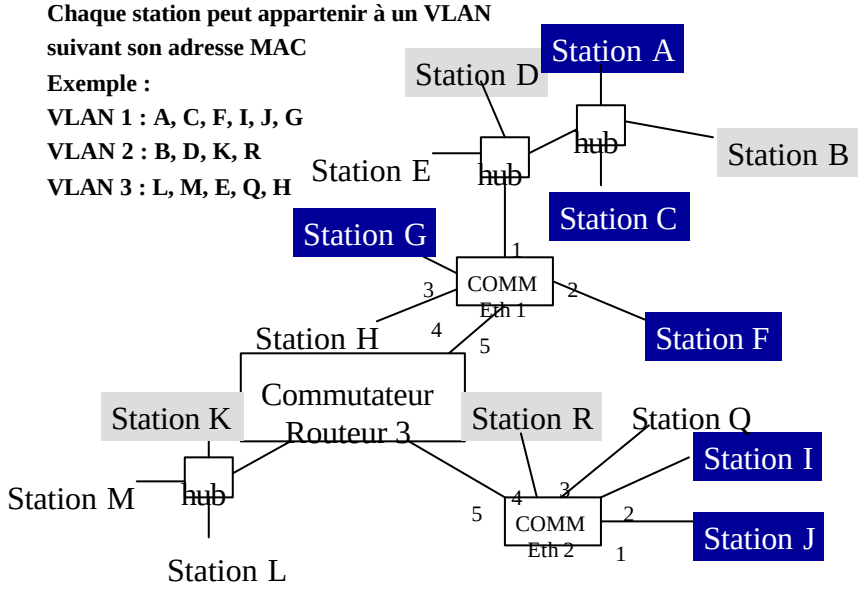
Chaque station peut appartenir à un VLAN suivant son adresse MAC

Exemple :

VLAN 1 : A, C, F, I, J, G

VLAN 2 : B, D, K, R

VLAN 3 : L, M, E, Q, H



Réseaux virtuels : VLAN par @ MAC

- **Configuration VLAN de Eth 1 : 3 VLANS 1-2-3**
  - **VLAN 1 : @ MAC de A, C, F, G**
  - **VLAN 2 : @ MAC de B, D, Q, R**
  - **VLAN 3 : @ MAC de E, H**
  - **Quand Eth1 reçoit une trame de A (VLAN 1) :**
    - Envoie vers port 2 (et port 5 : cf après)
- **Configuration VLAN de Eth 2 : 3 VLANS 1-2- »**
  - **Port 1 = VLAN 1** **Port 3 = VLAN 3**
  - **Port 2 = VLAN 1** **Port 4 = VLAN 2**
  - **Port 5 = Voir après**
  - **Quand Eth1 reçoit une trame de I (VLAN 1) :**
    - Envoie vers port 1 (et port 5, cf après)
- **Configuration commutateur de Eth1 (idem Eth2) :**
  - **Port 1 : @ MAC A, B, C, D, E**
  - **…**

VLAN par port ou par @ MAC

- **Avantages VLAN @MAC / port**
  - **Des stations sur des hubs peuvent appartenir à différents VLANs**
    - Mais la diffusion n'est pas sélective selon les branches des hubs
  - **On peut avoir des stations qui sont déplacées (déménagement ou mobiles) sans besoin de reconfiguration**
  - **On peut identifier chaque station avec son numéro de carte Ethernet**
    - Sécurité accrue
    - Si adresse MAC inconnue : appartient au VLAN « visiteurs »
- **Désavantages VLAN par @ Mac**
  - **Administration plus lourde**
    - Répertorier et tenir à jour des tables avec toutes les adresses MAC
  - **Si utilisateur change sa carte Ethernet : modification de configuration**

Réseaux virtuels : VLAN niveau 3

- **Affecter les trames Ethernet dans un VLAN différent selon des champs que l'on trouve dans la trame :**
  - **Champ type Ethernet : protocole : IP, IPX, Appletalk, …**
  - **L'adresse IP origine : sous-réseau**
    - mais ce n'est pas du routage
  - **…**
- **Peut être utile quand de nombreux protocoles sont utilisés sur un même réseau**
  - **Support des « anciennes applications »**
  - **De moins en moins utile**

Réseaux virtuels : VLAN

- **Commutateurs :**
  - **Ils conservent leur fonction de base : commutation, sans diffusion inutile**
  - **Certains peuvent ne pas avoir de fonctionnalité VLAN**
  - **Dans les exemples précédents les commutateurs ont la fonctionnalité d'accepter plusieurs adresses Ethernet et VLAN par port : ce n'est pas toujours le cas**
- **Routeurs :**
  - **Peuvent supporter 802.1Q. Si non, il faut autant de cartes Ethernet que de VLAN pour que le routeur route les VLAN**
- **Ex de VLANs dans un laboratoire**
  - **1 / par équipe de recherche pour stations de travail individuelles**
  - **Administration (peut inclure la station de chaque secrétaire d'équipe de recherche)**
  - **Test : toutes les machines de test des différentes équipes**
  - **Serveurs locaux**
  - **Serveurs Internet**
  - **Visiteurs**

Réseaux virtuels : VLAN

- **Le travail d'administration de VLAN n'est pas négligeable !**
  - **Il faut bien connaître le réseau (et être plusieurs à le connaître : pb absence)**
  - **Il faut un outil d'administration**
- **Théorie : on peut utiliser des commutateurs de différents constructeurs : IEEE802.1Q**
- **En pratique : commutateurs homogènes**
  - **Avec un outil d'administration fourni par le constructeur**
- **Les VLAN sont des réseaux virtuels pour LAN**
  - **Pas pour MAN ou WAN**

Réseaux virtuels : ATM

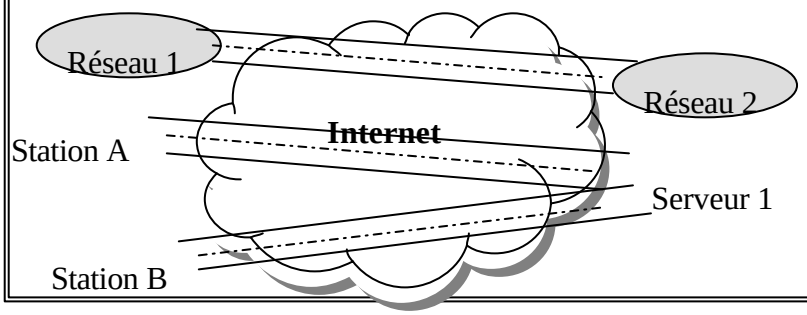
- **Interconnexion de réseaux Ethernet**
  - **ELAN : principe LANE (cf chapitre précédent)**
- **Utilisation de VPs ATM pour interconnecter des bâtiments (LAN) ou des sites (WAN) :**
  - **Réseaux Ethernet ou ATM**
  - **Réseaux IP**
  - **Fonctions :**
    - Sécurité : appelé aussi VPN ATM
    - Garantie de qualité de service (débit / VP)
  - **Exemple : service ATM de Renater**

Réseaux virtuels : VPN : but

- **VPN : Virtual Private Network**
  - **Terme générique qui regroupe plusieurs techniques**
- **Relier 2 réseaux distants (ou une station et un réseau) via un réseau ouvert (Internet) en garantissant :**
  - **Les services de VLAN pour IP : même réseau logique IP**
    - Etendre le réseau interne
  - **Des services des sécurité :**
    - Confidentialité des informations transmises
    - Intégrité des données (données non modifiées par un tiers)
    - Authentification de l'émetteur et du destinataire (au sens station ou routeur)
  - **Sans rechercher une qualité de service particulière (débit …)**
- **Eviter des infrastructures dédiées à base de LS**
  - **Réduction de coût en utilisant un réseau partagé**
- **Utilisation du tunneling (tunnelisation)**

Réseaux virtuels : VPN : tunnels

- **Un tunnel transporte des données entre 2 points sans que les éléments entre les points « perturbent » ce transport**
  - **Réseau de transport : transparent**
- **Entre 2 réseaux ou entre station-serveur**



Réseaux virtuels : VPN : tunnels

- **Encapsulation**
  - **En entrée de tunnel : données insérées (encapsulées) dans un paquet du protocole de tunnelisation**
  - **En sortie : données extraites : retrouvent leur forme initiale**
  - **Tunnel IP véhiculant des datagrammes IP**
    - Entête
      - @ IP Origine : @ IP entrée du tunnel
      - @ IP Destinatrice : @ IP sortie du tunnel
      - Protocole : tunnel : par ex : GRE
    - Données : datagramme initial IP
      - Entête : @ IP station origine - @ IP station destinatrice
      - Données
- **Plusieurs méthodes et protocoles**
  - **PPTP (RFC2637)**
  - **L2F (RFC2341)**
  - **L2TP (RFC2661)**
  - **IPSEC**

Réseaux virtuels : VPN : PPP

- **PPP : Point to Point Protocol**
  - **Permet de transporter des datagrammes IP sur une liaison point à point (RTC, LS par exemple)**
  - **Mais aussi d'autres protocoles que IP**
  - **Fonctionnalités supplémentaires :**
    - Authentification des extrêmités : PAP ou CHAP
      - Avant tout transfert de données
    - Chiffrement des données (confidentialité et intégrité)
    - Adressage IP dynamique
    - Compression
    - …

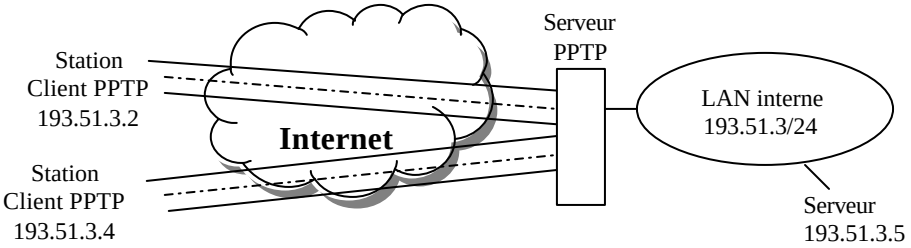
Réseaux virtuels : VPN : PPTP

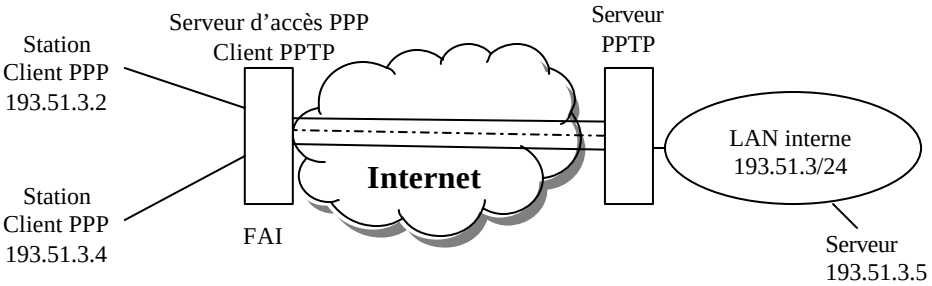
- **PPTP : Point-to-Point Tunneling Protocol**
- **Origine Microsoft**
- **VPN surtout sur réseau commuté pour accès particulier**
  - **Station isolée ✍ LAN entreprise**
- **Encapsulation IP, IPX, … ? PPP ? GRE ? IP**
  - **Pas uniquement IP**
- **La station isolée semble appartenir au LAN de l'entreprise**
  - **Elle peut avoir une adresse IP dans le sous-réseau IP du LAN, comme si elle était une station du réseau interne**
  - **Elle voit les autres stations du LAN comme si elle était connectée sur le LAN**
  - **Elle a les mêmes droits d'accès aux ressources du LAN qu'une station du LAN (serveurs de fichiers, imprimantes, …)**
  - **Elle utilisera la sortie Internet de l'entreprise pour accéder à l'Internet**

Réseaux virtuels : VPN : PPTP

- **Le chemin entre la station et le LAN est sécurisé**
  - **En utilisant les fonctions optionnelles de PPP**
  - **Authentification**
  - **Chiffrement**
- **Mais il faut bien configurer le serveur PPTP pour que des stations pirates ne puissent pas se connecter sur le LAN**
- **Serveur PPTP**
  - **Serveur NT, Linux, …**
  - **Serveur d'accès PPTP - Routeur**
- **Client PPTP**
  - **Windows NT, 95/98 …, Linux, Mac, …**

Réseaux virtuels : VPN : PPTP
2 utilisations





Réseaux virtuels : VPN : L2TP

- **L2TP : Layer 2 Tunneling Protocol**
  - **Réunion de PPTP et L2F (CISCO)**
- **Devrait remplacer PPTP**
- **3 cas de configuration possibles :**
  - **Tunnels L2TP : clients L2TP et serveur L2TP (idem PPTP)**
  - **PPP : clients PPP et FAI - Tunnels L2TP : FAI et serveur L2TP (idem PPTP)**
  - **LAN – Serveur L2TP – Tunnels L2TP – Serveur L2TP - LAN**
- **Sécurité**
  - **Utilisation possible des fonctions de PPP**
  - **Pour protéger le tunnel : IPSec**

Réseaux virtuels : VPN : IPSec

- **IPSec : IP Security Protocol**
- **IETF : Pour mettre un peu d'ordre dans les différentes méthodes de tunneling et de sécurisation**
- **Sécurisation des échanges au niveau IP**
  - **Chaque datagramme est authentifié et/ou chiffré**
- **Inclus dans IPv6 (intégré dans toutes les piles IPv6)**
- **Optionnel dans IPv4**
- **Evolution majeure de IP**
- **Peut-être mis en œuvre sur tout équipement IP**
  - **Routeur, serveur, station de travail, …**
- **Peut-être mis en œuvre de bout en bout ou sur un tronçon du chemin**

Réseaux virtuels : VPN : IPSec

- **Entêtes ajoutés :**
  - **AH : Authentication Header**
  - **ESP : Encapsulation Security Payload**
- **Datagramme avec AH**
  - **Entête IP – AH – (Entête TCP/UDP – Données) en clair**
- **AH (Authentication Header)**
  - **SPI : Security Parameter Index ✍ SA (Security Association)**
    - Index d'une table qui pointe sur tout ce qui est nécessaire au récepteur pour interpréter cette entête : algorithmes de crypto utilisés …
  - **Numéro de séquence**
    - Evite le rejeu du datagramme
  - **Signature électronique du contenu du datagramme (? entête IP)**
    - Checksum chiffré
    - Garantit intégrité et authentifie l'origine

Réseaux virtuels : VPN : IPSec

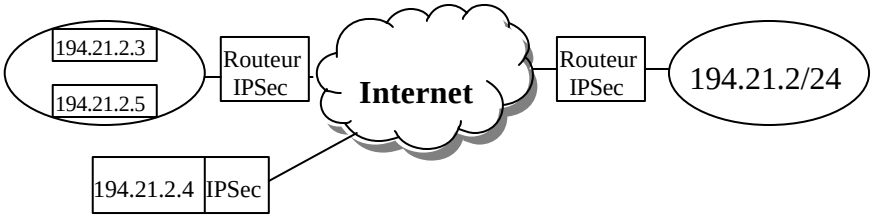
- **Datagramme avec ESP**
  - **Entête IP – Entête ESP – (Entête TCP/UDP – Données) chiffrés – [Authentication ESP]**
- **Entête ESP (Encapsulation Security Payload)**
  - **SPI : Security Parameter Index ✍ SA (Security Association)**
  - **Numéro de séquence**
- **Authentification ESP**
  - **Optionnelle**
  - **Signature – authentification : checksum chiffré : similaire AH**
    - AH inclut l'entête IP pas ESP
    - Utilisé en mode tunnel pour la signature (pas AH)
- **2 Modes d'utilisation**
  - **Mode transport**
  - **Mode tunnel**

Réseaux virtuels : VPN : modes IPSec

- **Mode transport**
  - **L'entête IP d'origine n'est pas contenue dans l'encapsulation**
  - **Entête IP – AH – Entête TCP – Données**
  - **Entête IP – ESP – (Entête TCP – Données) chiffrées**
  - **Entête IP – AH – ESP – (Entête TCP – Données) chiffrés**
- **Mode tunnel**
  - **Entête IP (nouveau) – AH – Entête IP (origine) - Entête TCP – Données**
  - **Entête IP (nouveau) - ESP - (Entête IP (origine) - Entête TCP - Données) chiffrées - [Authen ESP]**

Réseaux virtuels : VPN : IPSec tunnel

- **Le mode tunnel permet les fonctionnalités des VPN que l'on a vues :**
  - **Stations distantes ou sous-réseau distant considérés comme une partie du LAN (avec le même adressage)**
  - **Sécurité dans le transport**



Réseaux virtuels : VPN : IPSec-Sécurité

Security associations : SA

- **IPSec permet d'utiliser différents algorithmes, clés, … de cryptographie**
  - **Les 2 extrémités doivent se mettre d'accord**
- **Pour chaque connexion IPSec : 1 ou 2 SA**
  - **Une SA pour AH**
  - **Une SA pour ESP**
- **SA**
  - **Algo d'authentification (MD5, …)**
  - **Algo de chiffrement (DES, …)**
  - **Clés de chiffrement**
  - **Clés d'authentification**
  - **Durée de vie des clés**
  - **…**

Réseaux virtuels : VPN : IPSec

- **Gestion des clés**
  - **Manuelle**
  - **IKE Internet Key Exchange (ancien nom : ISAKMP)**
    - Procédure pour que les 2 extrémités se mettent d'accord : protocoles, algorithmes, clés
    - Management des clés : fourniture de clés de manière sécurisée …
- **IPSec**
  - **Très solide, bien conçu et intégré dans toutes les piles IPv6**
  - **Devrait beaucoup se répandre**
  - **Distinction Auth / Chiff : OK pour les législations**
  - **Mais attention : sécurité IP (pas utilisateur …)**

Services de FT : plan

- **LS (transfix), RNIS (numeris), ADSL : cf avant**
- **Interconnexion niveau 2 « traditionnelle » moyen débit**
  - **Frame Relay**
  - **Transrel**
- **Interconnexion niveau 2 haut-débit**
  - **Turbo DSL**
  - **Intra-Cité**
  - **Inter LAN**
  - **SMHD**
  - **SMHD - Giga**
  - **MultiLAN**
- **Services IP (pour entreprises)**
  - **Les Classiques Oléane**
  - **Global Intranet**
  - **Global Extranet**
  - **Collecte IP/ADSL**

Services FT : interconnexion « traditionnelle » moyen débit

- **Frame Relay**
  - **Remplacement de X25 : réseau commuté commuté avec circuits virtuels**
  - **Débits de 19.2 Kb/s à 8 Mb/s**
  - **Connexion réseaux FR d'entreprise**
  - **Réseau international**
- **Transrel**
  - **Service point à point**
  - **Interconnexion de réseaux Ethernet, Token Ring**
  - **Interfaces (équipements : ponts)**
    - Ethernet 10 ou 100 Mb/s
    - Token Ring 4 ou 16 Mb/s

Services FT : interco HD : Turbo DSL

- **Même zone (géographique)**
- **<u>Agences ou particuliers ✍ Site central</u>**
- **Liaisons permanentes**
- **Raccordement site central**
  - **ATM 30, 60, 90 ou 120 Mb/s**
- **Raccordement extrémités**
  - **ADSL jusqu'à 2 Mb/s – 320 Kb/s**

Services FT : interco HD : Intra-Cité

- **MAN : Voix et données**
- **Boucle locale FT**
- **Connexions point à point (LS virtuelles) de 2 sites équivalents à 2 Mb/s, 10 Mb/s ou 100 Mb/s**
- **Interfaces**
  - **G703 : PABX : 2 Mb/s**
  - **Ethernet 10 ou 100BaseT : 2 Mb/s, 10 Mb/s, 100 Mb/s**
- **Connexion entreprise**
  - **PABX, routeur IP, commutateur Ethernet**

Services FT : interco HD : Inter LAN

- **MAN : données**
- **Client : PME (petit budget)**
- **Connexions point à point (LS virtuelles) ou multipoint de sites équivalents à 2, 4, 20, 40, 60, 100 Mb/s**
- **Interfaces**
  - **Ethernet 10 ou 100BaseT ou GigaEthernet**
  - **ATM**
- **Différents niveaux de « qualité de débit »**
  - **Débit minimum garanti (on peut avoir plus si réseau peu chargé)**
  - **Débit permanent garanti**
  - **Débit non garanti (?)**
- **Connexion entreprise**
  - **Routeur IP, commutateur Ethernet, commutateur ATM**

Services FT : interco HD : SMHD

- **MAN : <u>n sites</u>**
- **SMHD : Service Multisites Haut-débit**
  - **Protocole SMDH**
  - **Boucle FO MAN dédiée à 155, 622 ou 2.5 Gb/s**
  - **Sécurisation : chaque site est raccordé avec 2 parcours différents**
- **Les sites se partagent la bande passante de la boucle**
- **Liaisons permanentes ou temporaires entre sites**
  - **2, n x 2, 34, 45 ou 155 Mb/s**
- **Interfaces**
  - **G703, Ethernet 10 et 100 Mb/s**

Services FT : interco HD : SMHD Giga

- **Nouveau**
- **MAN – 3 sites minimum**
- **Technologie DWDM**
  - **Multiplexage optique**
  - **Ce n'est donc pas le protocole SMHD**
- **Liaisons (jusqu'à 32 par lien)**
  - **622 Mbps ✍ 2.5 Gigabit/s**
  - **<u>Très hauts débits</u>**
- **Interfaces d'accès**
  - **Fast Eth, Giga Eth, Fiber Channel, ..**
- **Bientôt 10 Gigabit/s**

Services FT : interco HD : MultiLAN

- **WAN : 92 villes françaises et aussi international**
- **Raccordements (physiques) : 2, 34 ou 155 Mb/s**
- **Connexions point à point (LS virtuelles) de débits de 256 Kb/s à 100 Mb/s**
- **Interfaces**
  - **ATM**
  - **Ethernet 10 ou 100BaseT**
  - **…**
- **Infrastructure de réseau FT : ATM**
- **Connexion entreprise : PABX, commutateur ATM, équipement vidéo, routeur IP, commutateur Ethernet**
- **Applications : voix (PABX), données (LAN), vidéo**

Services FT : IP : Classiques Oleane

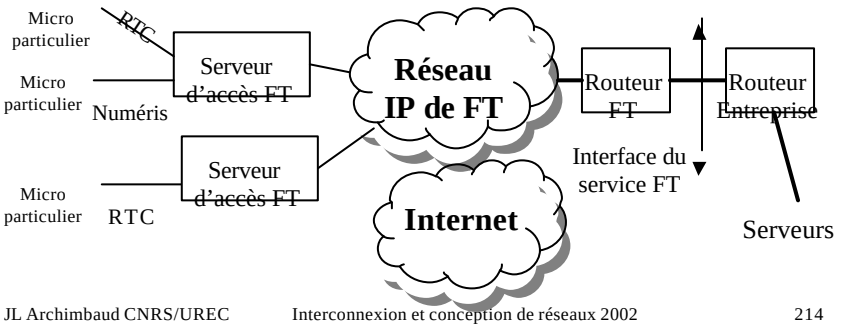
- **Connexion Entreprise à Internet**
- **Types de raccordement**
  - **Lien permanent avec possibilité de back-up Numeris**
  - **Connexion RTC, Numeris, GSM**
  - **ADSL**
- **Equipement de connexion**
  - **Routeur IP fourni ou non**
- **Services à valeur ajoutée**
  - **Adresses IP**
  - **Hébergement, gestion DNS, serveur Web**
  - **Boites aux lettres (anti-virus possible)**
  - **Proxy Web**
  - **….**

Services FT : IP : Global Intranet

- **Créer un réseau privé virtuel pour l'entreprise**
  - **Sites : moyen débit**
  - **Postes utilisateurs fixes ou mobiles : bas débit**
- **Techniques**
  - **CV ATM**
  - **Filtrage adresses IP**
  - **Tunelling IP**
  - **Authentification des utilisateurs**
- **Equipements de connexion**
  - **Routeur fourni ou non**
  - **Poste utilisateur**
- **Accès**
  - **Permanent 64 Kb/s ✍ 2 Mb/s**
  - **Commuté : RTC, Numeris, GSM**
  - **ADSL**

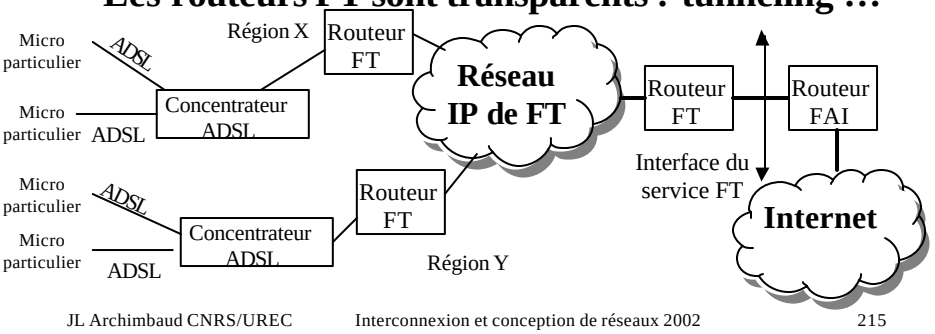
Services FT : IP : Global Extranet

- **Service d'information de l'entreprise (Extranet) accessible par RTC ou Internet**
  - **Clients, Partenaires, Fournisseurs**
- **Facture : téléphone particulier**
  - **Numéros d'appel réservés**
- **Technique : tunnels IP**



Services FT : IP : collecte IP/ADSL

- **Pour les fournisseurs d'accès Internet (FAI)**
- **<u>Pour collecter le trafic des abonnés ADSL</u>**
- **Routeur FT chez le FAI**
  - **Interfaces Ethernet 10, 100 ou 1000 Mb/s**
  - **Débits : 10 Mb/s ✍ 4 Gb/s**
- **Les routeurs FT sont transparents : tunneling …**



Services à assurer : plan

Services « obligatoires » à assurer (couche 7)

Uniquement aspect architecture – choix - stratégie

- **Noms (machines)**
  - **Principes**
  - **Plan de nommage**
- **Messagerie**
- **Annuaires**
- **Services Web**

Services : noms

- **Buts techniques**
  - **Traduction : nom de machine ✍ adresse IP**
  - **http://www.inpg.fr ✍ datagramme IP :**
    - Ouverture connexion TCP sur port 80
    - Adresse IP destinataire : ?
    - Comment : www.inpg.fr ✍ 195.83.76.58 ?
  - **Ping www.inpg.fr**
    - Datagramme ICMP - @ destination 195.83.76.58
  - **Dans l'autre sens aussi : @ IP ✍ nom de machine**
    - Configurations, contrôles d'accès, fichiers de trace, … explicités avec des noms
  - **Mais aussi messagerie électronique**
    - jla@urec.cnrs.fr ✍ serveur messagerie SMTP mail.urec.cnrs.fr

Services : noms

- **Pour que cela fonctionne dans l'Internet**
  - **Noms uniques**
  - **Système très solide : des serveurs DNS « direct» et « reverse »**
  - **Dynamique : ajout de noms décentralisé dans les serveurs DNS**
- **Unicité**
  - **Nommage hiérarchique arborescent avec des domaines**
    - .com, .edu, .org, …, .fr, .de, .uk, …
  - **Plan de nommage dans les organismes-entreprises**
- **Solidité – Dynamique**
  - **N serveurs de noms administrés localement**
    - Un serveur primaire par zone
    - Plusieurs serveurs secondaires
    - Copies régulières des informations primaire ✍ secondaires
  - **Caches**
    - Postes de travail
    - Serveurs (primaires – secondaires)
  - **Serveurs DNS : machines dédiées, aux bons emplacements**

Services : plan de nommage

- **Choix du nom de domaine (pour une entreprise)**
  - **Pas technique : image de l'entreprise**
    - Serveurs Web, …
    - Adresses électroniques
    - Un nom a maintenant une valeur commerciale
  - **Sous .com**
    - Quelques $
    - Pas de vérification
  - **Sous .fr**
    - Plusieurs dizaines (centaines) d'euros
    - Vérifications
    - AFNIC : association ✍ système « sain »
  - **Dérives**
    - Réservation de noms tels que cnrs.com pour revente
    - Certains pays (en voie de développement) :
      - Société à but uniquement lucratif qui gère le top level domain du pays

Services : plan de nommage machines

- **Choix de sous-domaines : technique**
  - **Un sous-domaine**
    - ✍ un serveur DNS « direct »
    - ✍ un administrateur
  - **Un serveur DNS « reverse »**
    - ✍ un sous-réseau IP
    - ✍ un administrateur
  - **On regroupe souvent serveur « direct » et « reverse »**
    - Quand ajout de machine : MAJ des 2 nécessaire
  - **En cas de problèmes : facilité de localisation**
    - Nom ✍ Où ?
  - **Possibilité d'alias sur les noms**
    - Très souple

Services : plan de nommage machines

Exemple : UREC (Paris, Grenoble, Lyon, Marseille)

- **Domaine urec.cnrs.fr**
  - **Sous-domaines grenoble.urec.cnrs.fr et paris.urec.cnrs.fr**
- **Un serveur DNS Paris (un administrateur)**
  - **Primaire : urec.cnrs.fr, paris.urec.cnrs.fr, reverse réseau IP Paris**
  - **Secondaire : grenoble.urec.cnrs.fr, reverse réseau IP Grenoble**
- **Un serveur DNS Grenoble (un autre administrateur)**
  - **Primaire pour grenoble.urec.cnrs.fr, reverse réseau IP grenoble**
  - **Secondaire : urec.cnrs.fr, paris.urec.cnrs.fr, reverse réseau IP Paris**
- **Lyon, Marseille : nommage machines laboratoires locaux**
- **Alias dans DNS urec.cnrs.fr, …**
  - **www.urec.cnrs.fr ✍ www.paris.urec.cnrs.fr : visibilité**
  - **Idem autres services : mail, …**
  - **Autres services dans domaine services.cnrs.fr ✍ urec.cnrs.fr**

Services : plan de nommage machines

- **Exemple : IMAG (fédération de 8 laboratoires)**
  - **Domaine imag.fr - pas de sous-domaine**
  - **Un serveur DNS primaire imag.fr**
  - **N serveurs DNS secondaires imag.fr**
    - Pour l'extérieur (authoritative) : 3
    - En interne, au moins un par laboratoire
  - **Equipe d'administrateurs soudée**
    - Choix des noms de toutes les machines centralisé
    - Bases de données mise à jour par chaque administrateur de labo
      - Script de mise à jour automatique du DNS primaire
  - **Serveurs Web de labo : nom du labo le nom : image**
    - www.imag.fr, www-id.imag.fr, www-clips.imag.fr, …
  - **Choix pas de ss-domaine ✍ visibilité de la fédération**
    - Une autre possibilité aurait été : un sous domaine par laboratoire

Services : plan nommage machines

- **Choix**
  - **Divers : image, organisation entreprise, organisation des administrateurs, histoire, …**
  - **Qu'ils soient clairs : document de référence :**
    - Comment est-ce organisé ?
    - Qui fait quoi ?
- **Visibilité / extérieur**
  - **Pour les noms des serveurs**
  - **Pour le nom des stations clientes : intérieur : choix technique**
- **Adressage privé - NAT**
  - **2 nommages : 2 DNS : interne – externe**
  - **Les noms de stations internes ne sont plus visibles de l'extérieur**
  - **Mais il faut néanmoins que les stations internes communiquent entre elles : document de référence toujours utile**
- **Les FAI offrent des services de DNS**
- **Pb : quand rachat … entreprise ✍ changement de nom ?**

Services : messagerie

- **Messagerie Internet : protocole SMTP**
  - **Messagerie interne dans l'entreprise peut être différence : passerelle nécessaire**
  - **Dans ce chapitre : messagerie interne SMTP, logiciel Sendmail ou Postfix**
- **Plan**
  - **Choix de la forme des adresses**
  - **Répartition des serveurs**
  - **Méthodes d'accès aux boites aux lettres**
  - **Format des messages**

Services : messagerie : adresses

Adresses de messagerie : quelle stratégie ?

- **De préférence forme canonique : Prénom.Nom@…**
  - **Exemple : Jean-Luc.Archimbaud@urec.cnrs.fr**
  - **Avantages**
    - Adresse unique (sauf homonymes)
    - Adresse « parlante » : peut éviter un annuaire
- **Faire apparaître sous-domaines ou non ?**
  - **Pierre.Durant@etudes.edf.fr ou Pierre.Durant@edf.fr ?**
  - **Pérennité de l'adresse et forme simple / centralisation**
- **Utiliser des adresses génériques**
  - **webmaster@.., postmaster@…, info@…, …**
  - **Peut-être pour des fonctions : direction@…, secrétariat@…, …**
  - **Avantage : pérennité quand la personne change de fonction**

Services : messagerie : adresses

- **« Transformation » d'adresses - redirection**
  - **Différents mécanismes peuvent modifier les champs « To» et « From » sur les messages arrivants ou partants**
  - **Serveurs-relais de messagerie : messages arrivants**
    - To : Francis.Duval@edf.fr ✍ Francis.Duval@der.edf.fr
  - **Serveurs-relais de messagerie : messages partants**
    - From : jla ✍ From : Jean-Luc.Archimbaud@urec.cnrs.fr
  - **Comptes utilisateurs : .forward (messages arrivants)**
    - To : jla@imag.fr ✍ To : Jean-Luc.Archimbaud@urec.cnrs.fr
  - **Ne pas en abuser**
    - Doit simplement résoudre les cas particuliers
- **Différencier adresse professionnelle et personnelle ? (au travail)**
  - **Problème : correspondance privée : débat non tranché**
- **« Cacher » les adresses pour limiter les SPAM ?**

Services : messagerie : serveurs

- **2 services à assurer :**
  - **Relais de messages et hébergement de boites aux lettres**
- **Entrant : un seul serveur relais avec les boites aux lettres**
  - **Accessible depuis l'Internet**
  - **Avec machine back-up quand indisponible**
    - DNS : plusieurs MX records
  - **Problème de sécurité : attaque des boites aux lettres**
- **Entrant : un serveur relais sans boite aux lettres**
  - **Accessible depuis l'Internet**
  - **Redirige vers 1 ou plusieurs serveurs internes suivant l'adresse du destinataire :**
    - Si adresses avec sous-domaine ✍ le serveur interne du sous-domaine
    - Sinon, base de données : une adresse ✍ son serveur interne
  - **Boites aux lettres sur serveurs internes**
  - **Serveurs internes non accessibles depuis l'Internet**
- **Sortant : préférable de passer par un seul serveur relais**
  - **Canonisation des adresses, surveillance, traces, …**

Services : messagerie : serveurs relais

- **Service à surveiller de près**
  - **Très souvent attaqué**
  - **Trace des abus**
- **Interdire le relayage : @ externe ✍ @ externes**
  - **Problème SPAM : obligatoire**
- **Installer un anti-virus**
  - **Evite MAJ sur chaque poste interne**
- **Lutter contre le SPAM**
  - **Outils avec mots clés et/ou black lists (pas de solution miracle)**
  - **La solution est la signature électronique**
- **Lutte anti-virus - SPAM : accord du personnel nécessaire**
- **Exemple IMAG**
  - **Un relais de messagerie externe (reçoit To : X@imag.fr)**
  - **N serveurs de messagerie internes avec boites : 1 / labo**
  - **Table : @ d'une personne ✍ serveur de messagerie interne**
  - **Gestion idem DNS**

Services : messagerie : accès aux boites

- **Connexion interactive sur le serveur**
  - **Qui contient les boites aux lettres : commande Mail Unix …**
  - **Pb : il faut gérer autant de comptes interactifs que de boites**
- **POP - Post Office Protocol**
  - **Accès depuis une station personnelle avec outil (navigateur, …)**
  - **Les boites aux lettres sont transférées sur la station personnelle**
- **IMAP - Internet Message Access Protocol**
  - **Accès depuis une station personnelle (navigateur, …)**
  - **Les boites aux lettres restent sur le serveur**
- **IMAP/POP ?**
  - **De plus en plus de IMAP**
  - **Dépend de l'utilisation :**
    - Veut-on garder sur le serveur les messages (place, sauvegarde, …) ?
    - Les utilisateurs sont ils connectés lorsqu'ils utilisent la messagerie ?
  - **Versions sécurisées : POPS – IMAPS**
    - Authentification ou non des clients

Service : messagerie : formats messages

- **MIME - Multipurpose Internet Mail Extensions**
  - **Standard pour format de messages contenant tous types de données : texte, video, voix, …**
- **S/MIME – Security …**
  - **Version sécurisée de MIME**
  - **Certificats électroniques**
  - **Signature électronique**
    - Authentification
    - Intégrité
  - **Chiffrement**
  - **Concurrent : PGP**
- **Principal pb messagerie : pas authentification expéditeur**
  - **SPAM, Virus, pas de valeur juridique, …**
- **Messagerie : service externalisable**

Annuaires : un standard

- **LDAP - Lightweight Directory Access Protocol**
  - **Communications client-serveur (sécurisées si voulu)**
  - **Modèle de données**
    - Arborescence hiérarchique
    - Classes d'objets
    - Nommage
  - **Modèle fonctionnel**
    - Recherche, comparaison, ajout, …
  - **API**
  - **Réplication**
  - **…**
- **Un annuaire LDAP**
  - **Peut utiliser un logiciel de base de données : oracle …**
    - LDAP : Interface standard d'accès

Annuaires LDAP : utilisations

- **Classique de personnes : adresses électroniques**
  - **Accès avec navigateur – complétion d'adresse**
  - **Gestionnaire de liste de diffusion, …**
- **De certificats électroniques**
- **De droits d'accès**
  - **A des systèmes, des applications, …**
  - **Remplacement de NIS, NIS+**
- **De ressources**
  - **Grilles de calcul**
  - **Equipements (réseau)**
- **Besoin d'avoir une réflexion sur l'architecture**
  - **Un seul annuaire ou n / utilisation ou groupe**
  - **Séparer LDAPs publics et privés (internes)**
  - **Sécurisation de l'annuaire, pb de SPAM (limitation du nb d'accès), …**

Services Web

- **Accès aux serveurs Web externes (Internet)**
  - **Autorisation ou non ?**
    - Décision de direction, pas d'administrateur réseau
  - **Proxy ou non ?**
  - **Attention aux problèmes de sécurité**
    - Virus dans documents récupérés
    - Exécution de code localement : javascript, …
    - ✍ Proxy utile
- **Serveurs Web de l'entreprise**
  - **Différencier administration technique / contenu**
  - **Définir les droits d'accès et une méthode de mise à jour**
  - **Pour Intranet**
    - Informations internes
    - Serveurs dans un sous-réseau non accessible depuis l'extérieur
  - **Pour Extranet – Internet**
    - Information publiques
    - Serveurs dans un sous-réseau public

Fonctions «annexes » équipements actifs

PLAN

- **Administration**
- **Tunnels**
- **IPSec**
- **NAT**
- **Filtrage**
- **Multicast**
- **Gestion files d'attente**

Fonctions «annexes » équipements actifs

- **Administration**
  - **Agent SNMP**
  - **Traces ✍ syslog**
  - **Compteurs : charge, nb de datagrammes, de bytes, …**
- **Tunneling**
  - **Cf chapitre sur les réseaux virtuels : VPN**
  - **Dans les routeurs, stations IP**
  - **Pour sécurité mais aussi IPv6 dans IPv4, multicast dans unicast, …**
- **IPSec**
  - **Cf chapitre sur les réseaux virtuels**
  - **Dans les routeurs, stations IP**

Fcts «annexes » éqts actifs : NAT

- **NAT – Network Address Translation (traduction)**
- **Fonction dans routeur d'accès (entre site et Internet)**
- **Traduit les adresses IP**
  - **Modifie l'entête des datagrammes IP échangés avec l'extérieur**
  - **Dans les sens sortant et entrant**
- **Une station du site**
  - **Possède une adresse interne 10.1.1.2**
    - Elle est configurée avec cette adresse
    - Les machines internes communiquent avec elle avec cette adresse
  - **Connue de l'extérieur avec l'adresse 193.96.49.64 (@ externe)**
    - Les machines de l'Internet communiquent avec elle avec cette adresse
  - **Le système est transparent pour les stations**
    - Le routeur entre le site et l'Internet fait la traduction

Fcts «annexes » éqts actifs : NAT

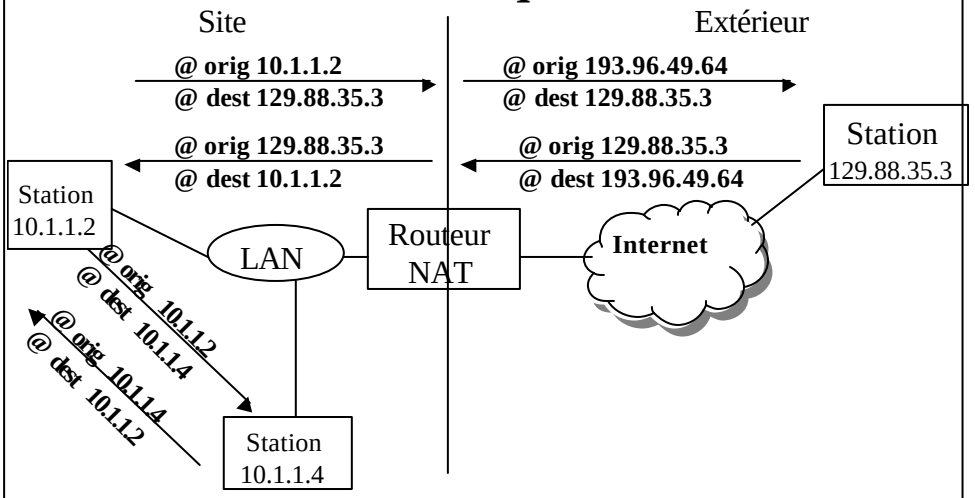


Table de traduction dans le routeur NAT
@ interne 10.1.1.2 ✍✍ @ externe 193.96.49.64

Fcts «annexes » éqts actifs : NAT

- **Traduction statique**
  - **10.1.1.2 ✍✍ 193.96.49.64**
  - **10.1.1.3 ✍✍ 193.96.49.66**
  - **…**
  - ✍ **Besoin autant d'adresses IP officielles que de stations**
- **Traduction dynamique**
  - **Pool d'adresses officielles (externes) pouvant être attribués**
    - Ex : 193.96.49.0/24
  - **Attribution d'une adresse externe lors du premier datagramme reçu par le routeur**
  - **Adresse libérée au bout d'un temps d'inactivité**
    - Ex : pas de datagramme avec cette adresse reçu depuis 3 heures
  - ✍ **On peut avoir plus de stations que d'adresses IP officielles**
- **On mixte : serveurs : statique - clients : dynamique**

NAT : PAT Port Address Translation

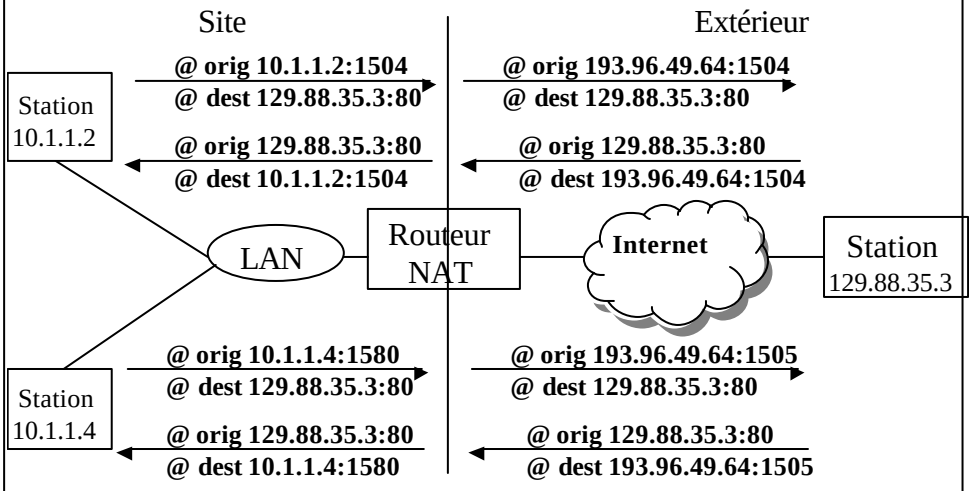


Table de traduction dans le routeur NAT (PAT)
@ interne 10.1.1.2:1504 ✍✍ @ externe 193.96.49.64:1504
@ interne 10.1.1.4:1580 ✍✍ @ externe 193.96.49.64:1505

Fcts «annexes » éqts actifs : NAT

- **Contenu de datagrammes (données) à modifier**
  - **Pour certains services :ICMP, FTP, H323, …**
- **Besoin de 2 serveurs DNS**
  - **Un interne : non accessible depuis l'extérieur**
    - Contient toutes les adresses internes
  - **Un externe : dans la DMZ**
    - Contient les adresses externes
  - **Les noms des stations clientes sont « aléatoires »**
- **Serveurs accédés depuis l'Internet**
  - **Adresses statiques**
- **L'adressage interne peut s'étendre sur n sites**
  - **Avec un VPN**
  - **Un routeur NAT pour communiquer avec l'extérieur**

NAT : pourquoi ?

- **On manque d'adresses officielles IP (4 bytes)**
  - **On ne peut plus numéroter toutes les stations IP de la planète de manière unique**
  - **En interne, sur les sites, numérote les stations avec les @ privées**
    - 10/8, 172.16/12, 192.168/16
    - Plusieurs sites peuvent utiliser les mêmes adresses
- **Exemple : site avec une @ réseau officielle 193.96.49.0/24**
  - **5000 machines internes**
  - **Numérote ses stations avec une adresse réseau privée : 10/8**
    - Peut numéroter des millions de machines
  - **Quelques adresses 193.96.49.0/24 réservées aux serveurs**
    - Accédés depuis l'Internet : DNS externe 193.96.49.1, Web externe 193.96.49.2, Mail 193.96.49.3 (avec PAT ce peut être le même numéro)
  - **Pool d'adresses 193.96.49.[4,254] disponibles (NAT)**
    - Attribuées dynamiquement aux stations locales quand elles communiquent avec l'Internet
    - 250 machines internes peuvent communiquer avec l'Internet simultanément : beaucoup plus si on utilise PAT

NAT : plus et moins

- **Avantages**
  - **On dispose d'un espace d'adresses énorme en interne**
    - Pas de limitation dans l'architecture des sous-réseaux
    - Pas de problème quand nouvelles stations à numéroter
  - **Les stations clientes ont des @ IP dynamiques**
    - Plus difficiles à attaquer : meilleure sécurité
- **Désavantages**
  - **Sécurité : les stations clientes sont « anonymes »**
    - Difficile de savoir quelle station interne a attaqué un site externe
  - **Contrôle d'accès / @ IP effectué sur certains serveurs**
    - Impossible sauf si traduction statique
  - **Rompt le principe IP de connectivité de bout en bout**
    - Peut avoir des effets de bord sur certaines applications
  - **Retarde l'arrivée de IPv6**

NAT : conclusion

- **De très nombreux sites l'utilisent**
  - **Peu universitaires car premiers venus sur Internet, ils disposent de beaucoup d'adresses officielles**
  - **Système très bien huilé maintenant**
- **NAT / DHCP**
  - **DHCP : autre manière d'économiser des adresses**
  - **Mais beaucoup moins d'économie que NAT**
    - DHCP : une station a besoin d'une adresse officielle dès qu'elle communique avec l'extérieur mais aussi avec l'intérieur
    - Pas de possibilité de PAT
  - **On peut faire les 2**
    - DHCP : pour ses fonctions de configuration dynamique
    - NAT : pour ses fonctions de traduction d'adresse

Fcts «annexes » éqts actifs : filtrage

- **Consiste à laisser passer ou non certains flux selon les informations trouvées dans**
  - **Les entêtes des trames Ethernet**
  - **Les entêtes des datagrammes IP**
  - **Les entêtes des segments TCP, UDP**
- **Ponts, Commutateurs**
  - **Filtrage de niveau 2**
  - **Sur le contenu des entêtes des trames Ethernet**
- **Routeurs**
  - **Filtrage de niveau 3**
  - **Sur les entêtes IP, TCP, UDP**

Filtrage : rappel trame Ethernet – IP

- **Entête Ethernet**
  - **@ Ethernet destination**
  - **@ Ethernet origine**
  - **Champ type : protocole : 0800 IP, 0806 ARP, …**
- **Entête IP**
  - **@ IP origine**
  - **@ IP destination**
  - **Protocole : 1 ICMP, 6 TCP, 17 UDP, …**
- **Entête TCP ou UDP**
  - **Numéro de port source (application station source)**
  - **Numéro de port destination (application station destination)**

Filtrage : niveau 2

- **Ponts – commutateurs / port**
  - **Sur les entêtes Ethernet**
- **Exemple : filtrer sur un port**
  - **Certains protocoles : Appletalk, IPX, …**
    - Car il n'y a pas de stations qui utilisent ces procotoles sur ce port
    - Diminue la charge du côté du port
      - Filtre les trames multicast ou broadcast de ces protocoles
    - Evite les erreurs
      - Des utilisateurs sans compétence qui pourraient lancer ces protocoles sur leur station et perturber les autres stations
  - **Certaines adresses Ethernet origine**
    - Stations trop bavardes, polluantes
  - **Certaines adresses Ethernet destination multicast, broadcast**
- **But principal : diminuer la charge**

Filtrage : niveau 3

- **Dans les routeurs**
  - **Sur les entêtes IP, TCP, UDP**
- **But principal**
  - **Sécurité (protection de stations, de services, de serveur)**
  - **Limitation des flux applicatifs (pas de chat, P2P, …)**
- **Deux politiques :**
  - **Par défaut : tout est autorisé (P1)**
    - On interdit ce que l'on ne veut pas
  - **Par défaut : tout est interdit (P2)**
    - On autorise ce que l'on veut
- **Deux types de filtrages**
  - **Sur les adresses IP (de stations ou de (ss-)-réseaux)**
  - **Sur les numéros de ports (applications)**

Filtrage : niveau 3

- **Filtrage sur @ IP de station ou de (ss-)réseau**
  - **Sens entrant (Internet ✍ Site) / @ IP destination**
    - P1 : interdit l'accès à des stations « à protéger »
    - P2 : autorise uniquement l'accès à certains serveurs (publics)
  - **Sens entrant / @ IP origine**
    - P1 : interdit l'entrée de datagrammes de stations dangereuses (black-list)
    - P2 : autorise l'accès que depuis certaines stations
  - **Sens sortant (Site ✍ Internet) / @ IP origine**
    - P1 : interdit à certaines stations de sortir (sur l'Internet, …)
    - P2 : autorise uniquement certaines stations à sortir
  - **Sens sortant / @ IP destination**
    - P1 : interdit l'accès à des serveurs à contenu peu recommandable
    - P2 : n'autorise l'accès que vers des serveurs répertoriés

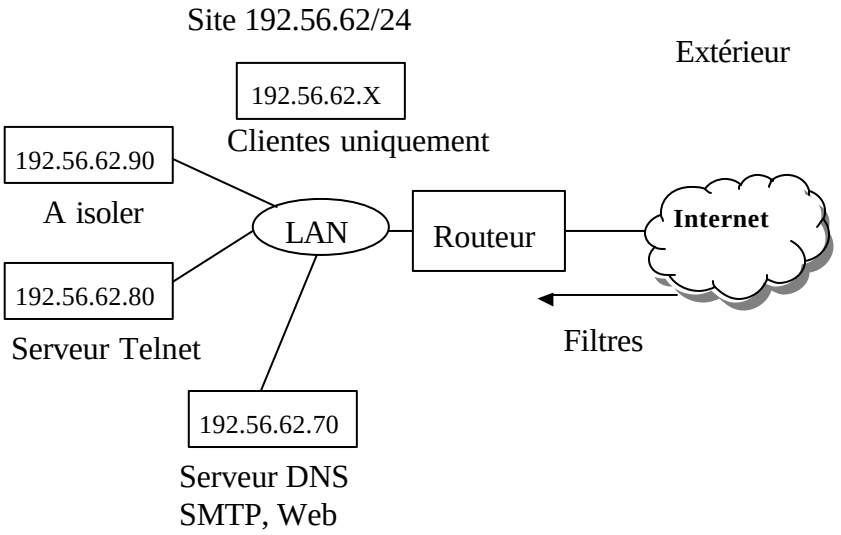
Filtrage : numéros de port

- **Applications IP : mode client –serveur**
  - **Serveur : wellknown ports**
    - HTTP : 80, Telnet : 23, SMTP : 25, …
  - **Client**
    - 1024, 1025, 1026, … pour FTP, Telnet, …
    - 1023, 1022, 1021 … pour rexec, rlogin, rsh, rcp, …
- **Exemples de filtre sens entrant (Internet ✍ Site)**
  - **P2 : Laisse passer uniquement les datagrammes avec port destination = 80 vers @IP destination 194.33.2.5**
    - Autorise uniquement l'accès HTTP sur le serveur Web 194.33.2.5
    - Si un autre utilisateur interne installe un serveur Web, il ne sera pas accessible depuis l'extérieur
  - **P1 : Filtre tous les datagrammes avec port destination = 23**
    - Interdit l'accès en telnet sur toutes les machines internes depuis l'extérieur

Filtrage : numéros de port

- **Exemple de filtre sens sortant (Site ✍ Internet)**
  - **P2 : laisse passer tous les datagrammes avec numéros de ports source > 980**
  - ✍ **Autorise toutes les stations à être cliente sur des serveurs Internet**
  - **P2 : laisse passer les datagrammes avec port dest=25 uniquement vers station 129.88.32.2**
  - ✍ **Oblige toutes les stations interne à passer par le relais de messagerie 129.88.32.2 pour envoyer du courrier**

Filtrage : exemple de politique



Filtrage : ex (simplifié) de politique 2

- **Les filtres sont exécutés en séquence (ACL CISCO)**
  - **Pour chaque datagramme**
    - Si condition remplie : action - exit
    - Sinon : continue les filtres
- **Si @ IP dest = 192.56.62.90 : filtre**
  - **Isole 192.56.62.90**
- **Si @ IP dest = 192.56.62.80 et port dest = 23 : laisse passer**
  - **Ouvre accès au serveur telnet : 192.56.62.80**
- **Si @ IP dest = 192.56.62.70 et port dest = (53 ou 25 ou 80) : laisse passer**
  - **Ouvre accès au serveur DNS, SMTP, Web 192.56.62.70**
- **Si port dest > 980 : laisse passer**
  - **Laisse passer le trafic vers stations clientes internes**
- **Reste : filtre**
  - **Interdit tous les autres trafics**

Filtrage : bilan

- **Les filtres peuvent être installés à l'intérieur du site**
  - **Sur les routeurs entre services, équipes, … par exemple**
  - **Entre sous-réseaux ou VLAN**
- **Avec l'Internet : politique 2 recommandée**
  - **On interdit tout sauf …**
  - **Si P1 : nouvelle vulnérabilité découverte ✍ MAJ des filtres**
- **Si fonction dans une boité dédiée avec interface graphique …✍ Garde-barrière**
  - **Fonction appelé « filtrage statique » dans les gardes-barrières**

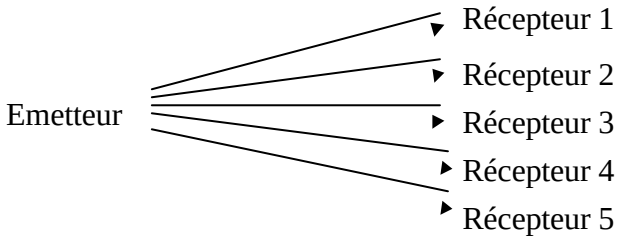
Filtrage : bilan

- **Filtrage dans les routeurs**
  - **Beaucoup utilisé en entrée de campus, laboratoires**
  - **En entreprise plutôt entre sous-réseaux internes**
    - En entrée (site-Internet) : garde-barrière
- **Limitations techniques**
  - **Basé sur des numéros de port : les applications peuvent utiliser d'autres numéros que les wellknown port (pb cheval de Troie)**
  - **Rebonds applicatifs indétectables**
  - **Tunnels applicatifs non détectable (HTTP par exemple)**
  - **✍ filtrage statefull dans garde-barrière nécessaire**

Fcts «annexes » éqts actifs : multicast IP

- **Applications habituelles : unicast**
  - **Point à point**
  - **1 émetteur ✍ 1 récepteur**
    - Le récepteur devenant ensuite émetteur
  - **Adresses Ethernet et IP unicast**
- **Applications multicast**
  - **1 émetteur ✍ n récepteurs (diffusion ciblée)**
  - **Radio (plutôt broadcast)**
  - **Télévision**
    - Non cryptée : broadcast
    - Cryptée (Canal + …) : multicast
  - **Télé-séminaire, télé-réunion, vidéo-conférence, …**
    - Dans ce cas un récepteur peut aussi devenir émetteur

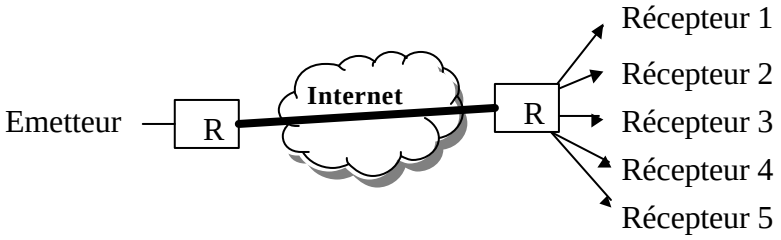
Multicast IP



- **Media idéal de transport : air**
  - **Ondes radio avec émetteurs terrestres, satellites, …**
  - **Pas de problème sauf partage des fréquences**

Multicast IP

- **Réseau filaire IP avec technique classique**
  - **On transporte n fois les mêmes données**
  - **On utilise beaucoup de bande passante**



- **Pour ne transporter qu'une fois les données :**
  - **Adresses, protocoles, routages, … multicast**

Multicast IP

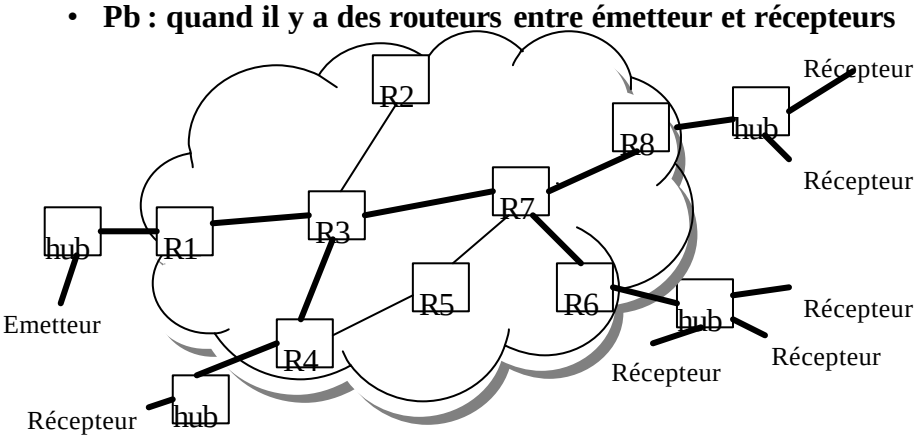
- **Participants à une appli multicast : groupe multicast**
- **Identification du groupe multicast : @ IP**
  - **Une adresse IP de classe D : 224.0.0.0 ✍ 239.255.255.255**
  - **Emetteur ✍ groupe : @ IP destination = @ IP multicast**
- **Choix d'une adresse multicast : statique**
- **Choix d'une adresse multicast : dynamique**
  - **Annuaire de groupes multicast en cours (ex : application SDR)**
  - **Responsable du groupe ✍ annuaire**
    - Je veux ouvrir une session « cours ARR » pour tel créneau horaire
    - Fournis moi une adresse multicast
  - **Annuaire**
    - Donne une adresse multicast au responsable : 224.2.0.1
    - Publie : « cours ARR » a telle @ multicast
  - **Participants au groupe**
    - Consultent annuaire et récupère l'adresse multicast du groupe

Multicast IP

- **Protocoles : UDP, RTP, RTCP (cf H323), …**
- **L'émetteur émettra ses données**
  - **Avec @ IP destination multicast : 224.2.0.1**
  - **@ IP origine : son @ IP (unicast)**
- **Les récepteurs se mettront à l'écoute**
  - **Pour recevoir les datagrammes avec cette @ dest**
- **Emetteur-récepteurs sur même réseau Ethernet**
  - **Utilisation du multicast Ethernet**
    - Premier octet de l'@ impair
    - IEEE a attribué 01.00.5E.X.Y.Z pour applications multicast IP
  - **@ Destination Ethernet : 01.00.5E.X.Y.Z**
    - IP : 224.2.0.1 ✍ Ethernet 01.00.5E.02.00.01

Multicast IP : routeurs

- **Pb : quand il y a des routeurs entre émetteur et récepteurs**



- **Les routeurs : @ dest 224.2.0.1 : que faire ?**
  - **R3 doit les renvoyer vers R4 et R7 mais pas vers R2**
- ✍ **tables de routages et protocoles de routage spécifiques**

Multicast IP : protocoles de routage

Protocole entre stations et premier routeur

- **Principe : stations : je veux m'abonner**
  - **Je veux recevoir le flux multicast 224.2.0.1**
  - **R4, R6, R8 vont recevoir ce message**
  - **R2 ne va pas le recevoir**
- **Exemple : IGMP**
  - **Internet Group Management Protocol**
  - **Le routeur émet un datagramme toutes les minutes**
    - Qui veut s'abonner à des groupes multicast ?
  - **Les stations intéressées répondent**
  - **Le routeur le redemande régulièrement**
    - Pour savoir si de nouvelles stations sont intéressées
    - Pour savoir si les anciennes abonnées sont toujours intéressées

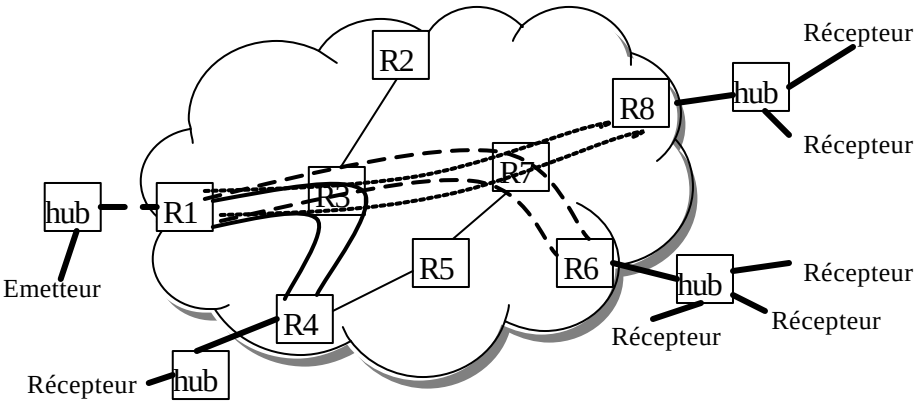
Multicast IP: protocoles de routage

Protocole entre routeurs
Exemple PIM Protocol Independant Multicast

- **But : arriver à un arbre de diffusion : 2 principes**
- **Dense mode**
  - **Les routeurs envoient à tous les routeurs tous les flux multicast**
    - Au départ. Exemple : R3 vers R4, R7, R2
  - **Les routeurs non intéressés demandent d'arrêter l'émission**
    - R2 indique à R3 : il y a personne chez moi d'intéressé par 224.2.0.1
    - R3 arrêtera d'émettre vers R2 ce flux : pruning
- **Sparse mode**
  - **Le routeur émetteur s'enregistre auprès du RP**
    - RP : Rendez vous Point
    - Je vais diffuser vers 224.2.0.1
    - Aucun routeur n'émet encore à ce stade
  - **Quand station intéressée : s'enregistre auprès du RP**
    - Celui-ci « avertit » les routeurs concernés d'émettre

Multicast IP

- **Quand partie du réseau non multicast : tunnels**
  - **Ex : uniquement les routeurs de sites R1, R4, R6 et R8 supporte le multicast (au cœur réseau d'opérateur)**



Multicast IP

- **Réseaux (routeurs) : complexe**
- **Travail d'opérateur : très important**
  - **En France uniquement Renater offre réellement ce service**
  - **On peut faire des tunnels**
- **Aujourd'hui**
  - **Beaucoup d'expérimentations autour du multicast**
  - **Réseau MBONE (opérationnel)**
  - **Télévision sur Internet : idée abandonnée**
  - **Radio sur Internet : pas multicast**
  - **Vidéoconférence : 3 solutions**
    - Multicast IP
    - H323
    - RNIS

Fcts «annexes » éqts actifs : gestion des files d'attente

- **Dans les routeurs : files d'attente**
  - **En entrée : généralement gérées basiquement**
  - **En sortie, pour chaque interface, choix :**
    - Taille de la file d'attente
      - Important car quand elle est pleine le routeur jette les datagrammes
    - La classification
      - Permet de faire passer en priorité certains datagrammes (voix / FTP par exemple)
- **Gestion des files d'attente : fondamental dans un réseau en mode non connecté (IP)**
- **Différentes techniques implémentées**
  - **FIFO**
  - **WFQ**
  - **PQ**
  - **CQ**

Gestion des files d'attente : FIFO

- **FIFO – First In First Out**
  - **Mécanisme simple :**
    - Une file d'attente / interface de sortie
    - Emission par ordre d'arrivée
  - **Plus : simple donc logiciels performants**
  - **Pas de problème quand réseau peu chargé et files d'attente de taille suffisante**
    - Pas de perte de datagramme
    - Temps de traitement (latence) court
  - **Dans le cas contraire**
    - Temps de traitement peut-être trop long pour certaines sessions TCP ou autre (par exemple s'il y a un gros transfert FTP en cours, il va bloquer le flux H323 d'une communication voix)
      - Perte de datagrammes (file d'attente pleine)
      - Latence trop grande
      - TCP ✍ retransmission, slow start, … : service très dégradé

Gestion des files d'attente : PQ

- **PQ : Priority Queuing**
- **Plusieurs files d'attente / interface de sortie**
  - **Une file par priorité**
  - **La file la plus prioritaire est envoyée avant les autres**
  - **Le routeur peut déterminer la priorité selon**
    - Le protocole niveau 3 : IP/IPX
    - Le protocole niveau 4 : TCP/UDP
    - Les applications : Telnet/FTP/H323/…
    - …
- **Pb : certains types de trafic (priorité trop basse) peuvent ne jamais être émis**
  - **Coupures de session, … : catastrophe**

Gestion des files d'attente : CBQ

- **CBQ : Class Based Queuing**
  - **Ou CQ - Custom Queuing**
  - **Amélioration du PQ**
- **Exemple : 3 files d'attente / interface de sortie**
  - **Haute, moyenne et basse priorité**
  - **A chaque « rotation » le routeur envoie 10 datagrammes de la file haute, 6 de ma moyenne, 3 de la basse.**
- **Evite que la basse priorité ne soit jamais émise**
- **Peut être une méthode pour partager une bande passante (entre classes de services)**
- **Pb : nécessite du CPU pour du très haut débit**

Gestion des files d'attente

- **WFQ : Weighted Fair Queuing**
  - **Modification du CBQ en prenant en compte le volume de données (nb de bytes) dans la répartition**
  - **Evite que les flux avec des gros datagrammes d'écrasent ceux avec des petits datagrammes**
- **Exemple d'efficacité de ces mécanismes**
  - **Expérience CISCO sur une liaison surchargée**
  - **Flux Telnet, FTP, Voix combinés sur un routeur**
    - Sans ces mécanismes : occupation bande passante 57 %
    - Avec ces mécanismes : occupation bande passante 98 %
- **Pb : réglage de ces mécanismes**
  - **Le constructeur fournit des exemples**
  - **Mais ça dépend de l'environnement : flux, …**

Fcts «annexes » éqts actifs : bilan

- **Les routeurs peuvent être très simples à configurer et administrer**
  - **Entre 2 Ethernet, avec uniquement la fonction de routage pour connecter un réseau de classe C avec l'extérieur**
  - **Une dizaine de lignes de configuration**
- **Mais aussi très complexes**
  - **Si on rajoute : comptabilité, tunnels, IPSec, routage dynamique, filtrage, NAT, multicast, files d'attente, …**
  - **Plusieurs centaines, voire milliers de lignes de configuration**
  - **Demande des experts : chaque ligne de configuration est importante**
- **Choix lors de l'achat d'un nouveau matériel**
  - **Tendance à prendre toujours le même constructeur**
    - Expérience, habitude des ingénieurs
  - **Attention au monopole**
  - **Des « Clones » d'OS de routeurs connus existent**

Qualité de service QoS (IP)

- **Internet (IP) de base : best effort**
  - **Le réseau peut avoir une mauvaise qualité (pertes, …) voire devenir inutilisable**
- **La QoS repose sur quelques paramètres techniques**
  - **Débit (bande passante)**
  - **Pertes**
  - **Latence (délai de transmission)**
  - **Variation de la latence : gigue ou jitter**

  Mais impossibles à garantir dans l'Internet entre 2 utilisateurs
- **QoS pour l'utilisateur : le réseau doit être transparent**
- **QoS où ?**
  - **Entre deux sites**
  - **Entre deux utilisateurs**
  - **Pour un type d'application ?**
  - **…**
- **2 standards (principes) pour Internet : RSVP et DiffServ**

Qualité de service (IP) : RSVP

- **RSVP : Resource Reservation Protocol**
- **Protocole en // de TCP, UDP**
  - **Comme ICMP et les protocoles de routage**
- **Principes**
  - **La station (réceptrice) demande une QoS au réseau (bande passante, …)**
  - **Tous les routeurs le long du chemin**
    - Prennent en compte cette demande et réservent les ressources nécessaires : CPU, mémoire, … (ils peuvent refuser)
    - Tiennent à jour une table avec toutes les réservations effectuées
- **Problème : (trop) complexe**
  - **Adapté au mode connecté, pas à IP**
    - Que se passe-t-il quand le routage est dissymétrique ou change ? …
    - Flux multicast ?

Qualité de service (IP) : Diffserv

- **Diffserv : Differentiated Services**
- **Les datagrammes sont marqués / contenu**
  - **Champ TOS dans IPv4, Traffic Class dans IPv6**
  - **Par la station / routeur d « entrée »**
- **Chaque routeur traite différemment les datagrammes**
  - **Mécanismes dans routeur : gestion files d'attente adaptée au champ TOS ou Traffic Class**
- **Simple mais peu précis**
  - **Peut être facilement implémenté**
  - **Là ou cela peut être utile (sur une partie du chemin)**
    - Liaisons à moyen, bas débits
    - Pour certaines applications

Qualité de service (IP)

- **Quand bande passante « à profusion » : QoS inutile**
  - **Le cas généralement des LAN**
  - **La bande passante disponible sur FO devient énorme**
- **Problème**
  - **Besoin de QoS quand la bande passante est limitée car chère c'est à dire dans les WAN**
  - **Or c'est le plus difficile car présence d'un opérateur et souvent même de plusieurs opérateurs**
- **Comment vérifier que le client respecte le contrat ?**
  - **Non traité dans ce cours : policy**
- **On ne pourra pas implémenter un mécanisme de qualité de service global dans tout l'Internet**
- **Les opérateurs utilisent plutôt des mécanismes « légers »**
  - **Sur certaines portions, pour certains clients/applications**
- **Entreprises : choisissent des équipements qui supportent DiffServ, au cas où …**

Administration de réseau : plan

- **Que faut il administrer ?**
- **Les hommes**
  - **Administrateurs et utilisateurs**
- **Les standards**
  - **SNMP …**
- **La configuration des équipements**
- **La surveillance**
  - **Détection des anomalies**
- **Le dépannage**
- **Les stations d'administration**
- **La sécurité**
- **La métrologie**
  - **Qui consomme quoi ? ✍ Comptabilité**
  - **Performances ✍ Evolution (anticiper)**
- **Remarques**

Administration de réseau : quoi ?

- **Que faut il administrer ?**
  - **Tout ce que l'on a vu, en particulier :**
- **Le câblage**
  - **Disposer des plans A JOUR**
  - **Garder les cahiers de recette**
  - **Disposer de valises de tests pour les grands réseaux**
- **Eléments d'interconnexion**
  - **Hubs, ponts, commutateurs, routeurs**
  - **Configuration, surveillance, métrologie**
- **Services (couche 7)**
  - **DNS**
    - Configurer, mettre à jour
  - **Relais et serveurs de messagerie**
    - Configurer, mettre à jour, surveiller (spool), métrologie
  - **…**
- **Sécurité**

Administration de réseau : les hommes

- **Constituer une équipe d'administrateurs**
  - **Qui fait quoi ? Sur quoi ?**
  - **Opérateurs – Techniciens – Ingénieurs – Gourous**
    - Faut il séparer très strictement les niveaux ?
      - Difficile car évolution des réseaux très rapide
    - Selon les stades d'installation : besoins différents de compétences
  - **Exemple entreprise : 3 équipes**
    - Infrastructure : câblage
    - Ingénierie : configuration équipements d'interco, services, routage
    - Supervision : surveillance, métrologie, sécurité
  - **Exemple opérateur Internet**
    - NOC : Network Operation Center : fait marcher
      - Configuration, surveillance, …
      - Procédures en cas d'incidents : tickets d'incidents, base de données, …
    - NIC : Network Information Center : interface avec les utilisateurs
      - Nommage, informations aux utilisateurs, hot line, …

Administration de réseau : les hommes

- **Où s'arrête le service d'administration réseau ?**
  - **Administration des serveurs Web ?**
  - **Installation des clients de messagerie sur les postes utilisateurs ?**
  - **….**
- **Astreinte ?**
  - **Selon les besoins de l'entreprise : cela coûte cher**
  - **Peut être externalisée**
- **Assistance (hot line) pour les utilisateurs**
  - **Ca ne marche pas !**
  - **Obligatoire**
  - **Centrale puis dispatching**
  - **Locale puis appel à l'assistance centrale si besoin**
  - **Difficile pour un utilisateur de séparer réseau / application**
- **Il faut une très bonne organisation humaine**
  - **Ne pas hésiter à décentraliser (noms, adresses, …)**
  - **Compétences : formation continue obligatoire**

Administration de réseau : standards

- **ICMP**
  - **Echo, TTL exceeded, Dest unreachable, redirect, …**
  - **Utilisé par les outils ping, traceroute par exemple**
  - **Avantage : supporté par toute station IP (ordi, routeur, …)**
  - **Peut sembler anodin mais en fait très utilisé**
- **SNMP - Simple Network Management Protocol**
  - **Agent (serveur) dans hub, commut, routeur, station, …**
  - **Manager depuis station d'administration**
  - **MIB : informations (@, …) – standard ou constructeur**
  - **Fonctions : GET – SET – TRAP sur UDP**
  - **Sécurité embryonnaire ✍ config ne se fait pas avec SNMP**
- **RMON – RMON2 : MIBs pour sondes**
- **Les standards permettent d'avoir un même outil pour administrer des matériels hétérogènes**

Administration de réseau : configuration des équipements

- **Avec telnet ou interface Web**
  - **Pas SNMP**
  - **Telnet est souvent plus précis (pour les spécialistes)**
  - **Attention aux mots de passe : ajouter filtrage / @ IP**
- **Perte de la configuration quand arrêt de l'équipement ?**
- **Stockage des différentes configurations**
  - **Généralement : TFTP**
    - Permet de sauvegarder une configuration sur un serveur
    - Inversement de charger cette configuration depuis ce serveur dans l'équipement actif
  - **Attention : pas de mot de passe dans TFTP**
- **Outils de constructeurs qui permettent de gérer plusieurs versions de configuration et d'OS …**

Administration de réseau : surveillance

- **But : détecter (rapidement) des anomalies**
- **2 types d'informations utiles**
  - **Alarmes : lien coupé, élément arrêté, daemon/service inactif, …**
  - **Relevés (courbes, tableaux, …) sur une courte période indiquant des charges, utilisations anormales (inhabituelles)**
    - Longue période ✍ métrologie
- **Transport : liens, équipements actifs**
  - **Traps SNMP émis par les équipements**
  - **Outils à base de ping et/ou traceroute depuis un point**
  - **Lors récupération de compteurs SNMP, sondes : courbes inhabituelles**
- **Services : messagerie, …**
  - **Daemon (service) inactif, spool plein, …**
  - **Ex d'outil : Big Brother**
    - Depuis une station interroge un daemon spécifique sur chaque machine de service
    - Détecte si service inactif, remonte des alarmes sur des seuils, …

Administration de réseau : surveillance

- **Alarmes et relevés**
  - **Arrivent sur ou partent de la station d'administration**
  - **Alarmes peuvent générer des mails … aux admins**
- **Des éléments de charges, activités anormales permettent de détecter des problèmes de sécurité**
  - **Brusque trafic vers une station, d'une application, …**
- **Les construire avec l'expérience**
  - **On peut récupérer énormément d'informations**
  - **Lesquelles sont pertinentes ?**
- **Les utilisateurs sont souvent plus rapides que les outils**
  - **Pour avertir : ça ne marche pas !**

Administration de réseau : dépannage

- **Où se situe le problème ? Quand localisé : réponse simple**
- **Faire preuve de logique**
  - **Première question : qu'est-ce qui a changé ?**
  - **Procéder par élimination**
- **Ex de démarche : telnet www.inpg.fr ne marche pas**
  - **Est-ce que la machine est accessible : ping www.inpg.fr ?**
  - **Si non, où s'arrête l'accès : traceroute www.inpg.fr ?**
    - Tout de suite : problème très local
      - Ping machine locale ✍ pb sur routeur sortant ou sur réseau local
      - Câblage ? Essai d'une prise voisine …
    - Si arrêt à un routeur : lequel ?
      - Sur le site distant : téléphone à l'administrateur distant …
      - Sur le site local
        - » Est-ce uniquement vers ce site : essaie d'atteindre un autre site de l'Internet
        - » …
    - …
  - **Si oui, service arrêté ? Problème de filtrage ?**
  - **…**

Administration de réseau : dépannage

- **Demande de connaître**
  - **La théorie : protocoles, fonctions des équipements, …**
  - **Son réseau, ses utilisateurs et leurs applications**
- **Analyseurs de protocoles**
  - **Quand vraiment on ne peut pas faire autrement**
  - **Ex de logiciel du domaine public : TcpDump**
  - **Station portable avec logiciel commercial**
  - **Il faut bien connaître les protocoles**
- **Problèmes logiciels : d'autres ont eu le même pb**
  - **Ne pas hésiter à utiliser les moteurs de recherche, news, …**

Admin réseau : station d'administration

- **Objectif : disposer d'UNE station qui**
  - **Permette de configurer tous les équipements et de stocker toutes les configurations**
  - **Reçoive toutes les alarmes (Traps SNMP, …)**
  - **Permette d'exécuter des scripts de surveillance développés, …**
  - **Dessine (automatiquement) la carte du réseau : liens, stations, équipements actifs, services**
  - **Affiche en rouge ce qui ne marche pas**
  - **Récupère des données de métrologie, les stocke, les affiche …**
- **Trois types**
  - **Stations « générales » (Sun, HP, IBM, …)**
    - Beaucoup de temps pour les maîtriser
  - **Stations de constructeurs d'équipements (CISCO)**
  - **Stations « artisanales » avec outils du domaine public**
- **Actuellement personne vise l'unicité (LA station)**
  - **Les grands sites ont les 3 types de stations précédentes**

Administration de réseau : sécurité

- **De plus en plus de problèmes de sécurité liés au réseau**
  - **Intrusion depuis l'Internet sur des machines internes**
  - **Attaque de serveurs Internet : Web, messagerie, DNS**
  - **Virus dans les messages électroniques, SPAM**
  - **Vers se propageant par le réseau**
  - **Spoofing d'@ IP, d'@ de messagerie**
  - **Charge de liens (trafic parasite) ✍ deny de service**
  - **…**
- **Organisation – coopération étroite entre responsable sécurité et administrateur réseau**
  - **Surveillance du réseau ✍ peut indiquer des problèmes de sécurité**
  - **Architecture de réseau ✍ permet d'appliquer facilement une politique de sécurité**
- **Maintenant la sécurité est un critère de choix important dans l'architecture et les équipements**

Administration de réseau : métrologie

- **But : répondre aux questions**
  - **A quoi sert le réseau ? A quelles applications ? A qui ? Quand ?**
  - **Qui l'utilise ? ✍ comptabilité si nécessaire**
  - **Y-a-t-il des goulots d'étranglement ? Des problèmes de performances ? ✍ Qualité de service**
  - **Quelle évolution ? ✍ Anticiper les besoins**
    - Commander l'augmentation de débit d'une liaison avant sa saturation
- **Ensemble de compteurs ✍ tableaux, courbes, …**
- **Qui fournit les informations ?**
  - **Equipements en écoute passive sur le réseau**
    - Sondes RMON, RMON2
    - Logiciel IPTrafic
    - Pb : nb d'équipements nécessaires, où les mettre (pb commutation)
  - **Equipements actifs du réseau : commutateurs, routeurs**
    - Comptent différentes choses ✍ compteurs spécifiques ou MIBs
    - Sont interrogés « par telnet » ou SNMP
    - Peuvent ne plus compter correctement quand d'autres urgences (charge)

Administration de réseau : métrologie

- **Quelles informations ?**
  - **Charge et taux de collisions / interface**
  - **Issues de comptage de différents champs des datagrammes**
    - @ IP (✍ numéros de réseaux), ports (✍ applications)
- **Exemples d'informations fournies**
  - **Le graphe journalier, hebdomadaire … de la charge de chaque brin Ethernet, de chaque liaison, du taux de collision**
  - **La répartition entre HTTP, MAIL, FTP, … sur chaque liaison**
  - **Les 20 stations les plus consommatrices**
  - **Le pourcentage de trafic intra-entreprise et extra-entreprise**
  - **Le pourcentage de bande passante de l'accès Internet consommé par chaque service de l'entreprise**
- **MRTG : logiciel graphique**
  - **Visualise le trafic sur les interfaces des commutateurs, routeurs, stations**
  - **Informations dans MIBs, obtenues par SNMP**

Administration de réseau : remarques

- **Fondamentale quand réseau d'envergure**
- **Surveillance :**
  - **Confidentialité des relevés**
  - **Respect de la vie privée**
- **Constats**
  - **Les équipements et les liaisons fonctionnent bien**
  - **IP est très solide**
  - ✍ **Conséquence négative sur le besoin d'administration**
- **Il faut se construire soi-même sa boite à outils**
  - **Pas une seule solution avec un seul produit**
  - **Difficile de conduire une approche théorique globale**
- **Beaucoup d'outils du domaine public existent**
  - **Mais chaque outil a un but particulier**
  - **Un administrateur doit bien savoir ce qu'il veut obtenir**

Administration de réseau : remarques

Exemple de choix de logiciels du domaine public

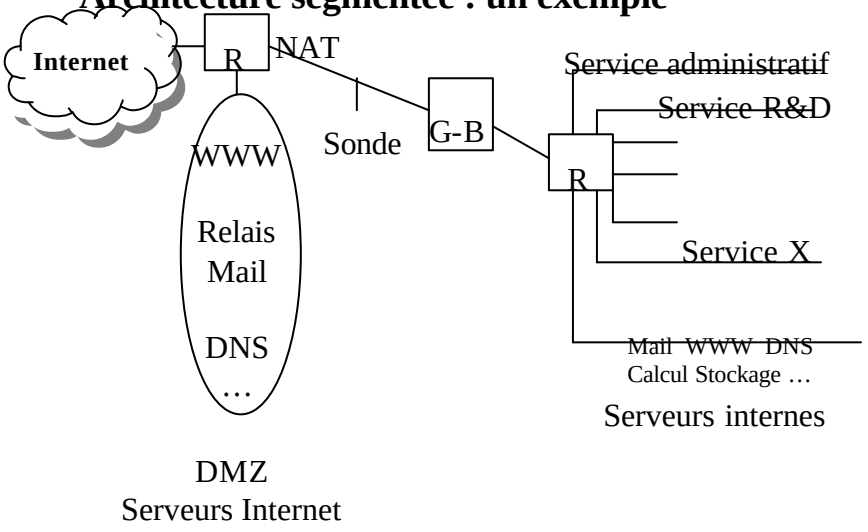
- **Outil de dépannage : tcpdump**
  - **Analyseur sur station Unix**
- **Outil de surveillance de liaison : MTR**
  - **Utilise ping et traceroute**
  - **Détecte rapidement une anomalie sur une liaison (coupure, engorgement). Sort des statistiques.**
- **Outil de surveillance de trafic : NTOP**
  - **Sonde**
  - **Indique à quoi est utilisé le réseau : charge, stations les plus bavardes, qui dialogue avec qui, avec quels protocoles, …**
  - **Sur une courte période**
- **Outil de surveillance de services : Mon**
  - **Services surveillés : messagerie, Web, FTP, SMTP, POP, IMAP, …**
  - **Alerte (mail) quand indisponibles**
- **Outil de métrologie : Cricket basé sur MRTG**
  - **Interroge des routeurs, commutateurs en SNMP**
  - **Charge, trafic sur une longue période**
- **Outil de métrologie orienté comptabilité : acct-cisco**
  - **Comptabilité (et répartition de charge) sur un routeur CISCO**

Eléments de sécurité

- **De protection contre les agressions externes en provenance de l'Internet (donc via le réseau)**
- **Garde-barrière**
  - **Equipement entre l'extérieur (hostile) et l'intérieur (de confiance) : routeur, équipement spécifique**
  - **3 ensembles principaux de contrôle**
    - Filtrage IP « de base » : cf cours sur les fonctions annexes des routeurs
    - Filtrage IP statefull : analyse des sessions applicatives
    - Relais applicatifs
      - Ex telnet : login sur garde-barrière puis login sur machine interne
      - Permet de concentrer les contrôles sur une machine
      - Difficile d'avoir des débits très élevés (Gigabits : non)
  - **Fiabilité : prévoir un équipement de secours**
  - **Entre réseau interne de l'entreprise et l'Internet**

Eléments de sécurité

- **Architecture segmentée : un exemple**



Eléments de sécurité

- **Un pb de cette architecture : travail à distance**
  - **Comment consulter son courrier à distance ?**
  - **Comment accéder à l'Intranet à distance ?**
  - **Solutions : cf connexion depuis l'Internet**
- **Un autre pb : portables**
  - **Où les connecter en interne (peuvent transporter des virus ou vers) ?**
- **Garde-barrière**
  - **Ne pas se reposer uniquement sur sa protection**
- **Sonde de détection d'intrusions**
  - **Sonde avec bibliothèque de signatures d'attaques**
- **Logiciel de simulation d'intrusions**
  - **Test de vulnérabilités à travers le réseau**
- **Rq : jamais de sécurité à 100 % (ne pas connecter ?)**

Accès à l'Internet (Web)

- **Station interne – LAN entreprise ✍ Internet**
- **Connexion directe (sans NAT)**
  - **@ IP officielle station ✍ @ IP serveur Web**
- **Connexion directe avec NAT**
  - **@ IP privée station ✍ @ IP serveur Web**
  - **NAT**
  - **@ IP officielle ✍ @ IP serveur Web**
- **Proxy-cache Web : serveur dans DMZ**
  - **@ IP station ✍ @ IP proxy Web**
  - **@ IP proxy Web ✍ @ IP serveur Web**
  - **2 sessions TCP (HTTP) : Station–Proxy et Proxy– Serveur Web**
  - **Cache, gain bande passante, filtrage, traces, anti-virus**
- **Sécurisé : 3ième méthode > 2nde > 1ère**
- **Accès à l'Internet : autorisation ou non aux salariés ?**

Accès depuis l'Internet

Serveurs Internet – Extranet de l'entreprise

- **Où les mettre ?**
  - **Dans la DMZ**
    - Zone Démilitarisée, semi-ouverte
  - **Chez un fournisseur d'accès ou hébergeur**
- **Stations dédiées**
- **Serveurs aux CNRS**
  - **Plutôt apache et Linux**
  - **Un peu IIS et Win-NT : bcq trop de pbs de sécurité**
- **Prévoir un mécanisme de MAJ**
- **Bien les sécuriser**

Accès depuis l'Internet

au réseau de l'entreprise

- **Comment travailler à distance ?**
  - **Consulter sa messagerie et émettre des messages**
  - **Accéder (interactif) aux stations internes**
  - **Transférer des fichiers**
  - **Accéder globalement à toutes les ressources de l'Intranet (réseau interne)**

  De manière sécurisée (pas de mot de passe en clair sur le réseau)
- **Consulter sa boite aux lettres**
  - **Accès interactif, POP, IMAP trop dangereux**
  - **SSL : POPS, IMAPS, Passerelle Web (HTTPS)**
    - Chiffrement uniquement
    - Chiffrement et authentification du client : certificat client
- **Emettre des messages**
  - **Relais « public » ou Sendmail-TLS**

Accès depuis l'Internet

au réseau de l'entreprise

- Accès interactif et transfert de fichiers
  - Sécurisation niveau application : SSH par exemple
  - Garde-barrière
- Accéder à toutes les ressources internes
  - VPN
  - PPT, L2TP, IPSec
- Tous ces mécanismes demandent des compétences pointues pour ne pas créer des trous de sécurité
- Personnel très mobile : tout sur le portable ?
  - Attention aux vols
  - Prévoir sauvegardes

Construire un réseau « solide »

Fiabilité, disponibilité, tolérance aux pannes, …

- Faire une architecture (physique et logique) simple
  - IP est très souple : ne pas abuser des possibilités pointues
- Faire des cahiers des charges (pour chaque évolution)
  - Qu'est-ce qu'on veut comme fonctionnalités ?
  - Laisser répondre les intégrateurs
- Choisir des équipements spécialisés
  - Un PC avec Linux n'est pas un routeur
- Ne pas hésiter à multiplier les machines dédiées /services
  - Web – FTP – Mail - DNS - …
- Services réseaux
  - Sous Unix ou sous NT ?
  - Selon compétences – habitudes – schéma directeur

Construire un réseau « solide »

- **Faire en fonction des moyens dont on dispose**
  - **Identifier ce qui est vital et non**
    - Cela va dépendre des applications
- **L'expérience est très utile**
  - **De chaque incident on tire une leçon**
  - **Il est difficile de travailler uniquement en théorie**
    - Ex de question : les équipements et les liaisons sont ils fiables ?
    - Comment le savoir sans expérience ?
    - Les routeurs par exemple sont jusqu'à présent très fiables
- **Faire appel aux entreprises du métier**
  - **Ne pas faire son câblage soi-même**
  - **Utiliser les services des opérateurs**
  - **…**
  - **Mais comprendre et contrôler (le domaine évolue vite)**

Réseau « solide » : disponibilité

- **Des liaisons**
  - **Chaque contrat avec opérateur garantit :**
    - Délai d'intervention
    - Délai de rétablissement : 4 h par exemple
    - …
  - **Etablir le même principe en interne**
    - Pb bien connu : « coup de pelleteuse »
- **Des équipements d'interconnexion (matériel)**
  - **Spare**
  - **Contrats de maintenance**
  - **Garantie : souvent à vie maintenant**
  - **Dans locaux réservés et protégés (accès, feu, climatisation ?, …)**
- **Des serveurs**
  - **Classique informatique**
- **Ces aspects sont très important (pbs engendrés graves)**
  - **Les informaticiens peuvent avoir tendance à le sous-estimé**

Réseau « solide » : tolérance aux pannes

- **Pannes**
  - **Rupture de liens**
  - **Arrêt d'équipements actifs et de services**
- **Liaisons (niveau 1)**
  - **Réseau maillé sur site**
    - Câbles mais aussi tranchées
    - Bâtiment : deux accès différents ?
  - **Liaisons externes LS**
    - 2 LS différentes ? : rare
      - Opérateurs : assurent le maillage
    - Back up par réseaux commutés : souvent
      - Débits inférieurs : est-ce que les applications fonctionnent toujours ? ✍ Est-ce utile ?
    - 2 points d'arrivées des liaisons externes différents ?

Réseau « solide » : tolérance aux pannes

Niveau 2 : difficulté : Ethernet = bus (✍ étoile)

- **Pas de structure d'anneau ou de maillage : pas de maillage possible en extrémité**
  - **(dans réseau capillaire : stations)**
  - **Sauf manipulation (changement de prise …)**
- **Au cœur : réseau maillé de commutateurs possible**
  - **Algorithme de Spanning Tree**
  - **Mais construction d'un arbre**
    - Un seul chemin utilisé à un moment
    - L'autre inutilisé : « gaspillage »

Réseau « solide » : tolérance aux pannes

Niveau 3 IP :

Routage dynamique sur réseau maillé de routeurs

- **Fonctionne très bien : permet de basculer d'un chemin à un autre sans intervention manuelle**
- **Pb (similaire à Eth) : à un instant une seule route vers une destination**
  - **On peut avoir 2 chemins différents pour une destination mais avec des poids différents**
    - Quand tout va bien : utilise le chemin avec le poids le plus fort
    - Bascule sur l'autre quand le premier chemin est coupé
    - Pas de répartition de charge / destination
  - **Mais on peut répartir plusieurs destinations entre des chemins différents**
    - Avec des poids différents permettant de basculer tout le trafic sur un chemin ou l'autre en cas de rupture d'un des chemins

Réseau « solide » : tolérance aux pannes

Services : serveurs secondaires

- **DNS : ce service doit être très fiable**
  - **Bien répartir les serveurs secondaires**
  - **Au moins un sur le même site**
    - Pas à côté du primaire (en cas de coupure de lien, …)
  - **2 autres ailleurs**
- **Messagerie (relais) : serveurs secondaires**
  - **DNS : MX records / domaine avec poids différents**
  - **Mécanisme supplémentaire de file d'attente sur serveur émetteur**
    - Reste 4 j par défaut si serveur distant ne répond pas
    - Mais c'est moins que la durée des périodes de fermeture des entreprises
- **Serveurs Web de l'entreprise**
  - **Si service important : image de marque, source de revenue, outil de travail (B2B) avec fournisseur/client …**
  - **Réplication de serveurs … : solutions commerciales disponibles**

Réseau « solide » : sécurité

- **Problème sécurité souvent très coûteux**
  - **Serveurs indisponibles, réseau bloqué, vols d'information, …**
  - **Or attaques viennent maintenant du réseau**
- **Outils imparfaits**
  - **Disparates (un peu à tous les niveaux …)**
  - **Ne colmatent qu'une partie des trous : toujours de nouveaux**
- **IP et Internet : conçus sans souci de sécurité**
  - **Principe d'un réseau global, égalitaire, sans frontière**
    - Pas conçu pour modèle réaliste : réseaux internes (entreprises) et un réseau d'interconnexion
  - **Pas de limitation de débit / station ou application**
  - **Transport en clair des informations (mot de passe donc)**
  - **Pas garantie émetteur dans messagerie électronique**
  - **…**
- **Actuellement la sécurité est une partie très importante du travail d'un administrateur de réseaux**

Réseau « solide » : qualité de service

- **Le réseau est vital pour toutes les activités**
  - **On « demande plus » au réseau**
    - Et à ses administrateurs
  - **Pas uniquement de garantir la connectivité**
    - Que le ping marche ne suffit plus
  - **Mais que les applications fonctionnent correctement**
- ✍ **Qualité de service**
  - **Savoir réserver des bandes passantes (avec certaines qualités) à**
    - Des utilisateurs (fonctionnellement à des sous-réseaux IP)
    - Des applications (fonctionnellement à des numéros de ports)
  - **Mécanismes**
    - Cf chapitres : files d'attente routeurs et QoS

La conception de réseaux

- **Assemblage de briques un peu disparates**
- **Mais l'architecte doit avoir une vision globale**
  - **Câbles ✍ applications**
  - **Connaissances dans des domaines très divers**
- **Le réseau demande un budget conséquent**
  - **Difficile à faire accepter à la direction**
  - **Arguments trop techniques**
- **Métier difficile**
  - **A risques**
    - Si le réseau ne marche pas ✍ catastrophe pour l'entreprise
  - **Forte évolution des technologies**
    - Remise à niveau continuel des connaissances
  - **Sens relationnel obligatoire**
    - Psychonet parfois
- **Mais intéressant …**

Etudes de cas : plan

- **Réseau de petit laboratoire éclaté : UREC**
  - **Réseau d'une PME sur 2 sites**
- **Réseau de campus**
  - **Réseau d'un gros site d'une entreprise**
- **Réseau Renater (national)**
  - **Réseau opérateur télécom**
  - **Réseau grande entreprise multi-sites**

Réseau UREC : stations Paris-Grenoble

- **Paris**
  - **7 personnes**
  - **5 bureaux, salle machines (climatisée)**
- **Grenoble**
  - **4 personnes + stagiaires**
  - **6 bureaux, salle machines (climatisée), local technique**
- **Choix OS**
  - **Stations personnelles : bureautique ✍ Windows**
  - **Serveur fichiers interne et sauvegarde ✍ Windows**
  - **Serveurs Internet (DNS, Mail, Web, …) ✍ Linux**
  - **Développement, tests ✍ Cela dépend**

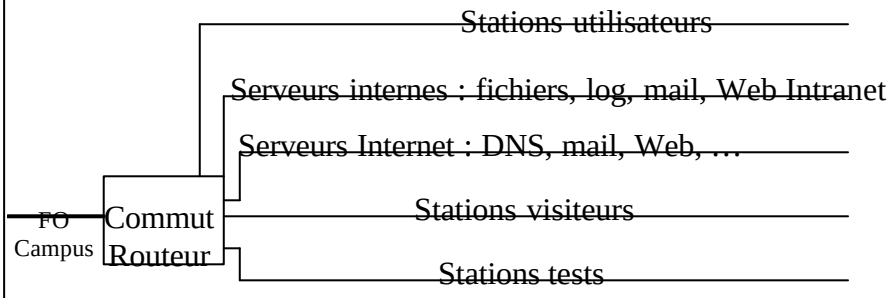
Réseaux UREC : câblage

- **Câblages effectués par 2 sociétés spécialisées**
  - **Cahier de recette : plans, repérage des prises, résultats tests**
- **TP catégorie 5 : 100 Mbps OK**
  - **Post-câblage à Grenoble**
  - **Pré-câblage à Paris (nouveaux bureaux)**
  - **Lors du déménagement Paris : abandon de la FO**
  - **3 prises par personne : 2 informatiques, 1 téléphone**
- **Cœur étoiles**
  - **Local technique à Grenoble, salle machine à Paris**
  - **Armoires de brassage**
- **Chemins de câble**
  - **Goulottes dans les bureaux et faux plafonds ailleurs**
- **Evolution à court terme**
  - **Bornes sans fil : portables, visiteurs**

Réseaux UREC

- **Equipements actifs**
  - **Paris et Grenoble : un commutateur routeur**
  - **2 ports FO Gbps Ethernet**
  - **48 ports TP 10-100 Mbps Ethernet**
  - **Contrat de maintenance**
  - **Avant : routeurs, commutateurs Ethernet et ATM, Hub Ethernet, Stations Eth et/ou ATM**
  - **Connexion extérieure : prise Giga Eth réseau de campus**
- **Plan d'adressage**
  - **1 numéro de classe C officiel à Paris**
  - **1 numéro de classe C officiel à Grenoble**
  - **Sous-réseaux sur les sites : utilisation des VLAN**

Réseaux UREC sur 2 sites : VLAN



- Autre possibilité : faire des VLAN étendus sur 2 sites
  - Pas vraiment de besoin (serveurs mail … dupliqués)
  - Trop de dépendance d'un site / l'autre (pb si coupure Renater par exemple)

Réseau UREC : noms machines (Rappel : déjà expliqué avant)

- Domaine urec.cnrs.fr
  - Ss-domaine grenoble.urec.cnrs.fr : toutes machines de Grenoble
  - Ss-domaine paris.urec.cnrs.fr : toutes les machines de Paris
- Alias
  - www.urec.fr ✍ elea.paris.urec.cnrs.fr
  - mail.urec.cnrs.fr ✍ thinos.paris.urec.cnrs.fr
  - …
  - services.cnrs.fr ✍ kaki.grenoble.urec.cnrs.fr
- Serveur DNS serveur Paris
  - Primaire urec.cnrs.fr et paris.urec.cnrs.fr
  - Secondaire grenoble.urec.cnrs.fr
- Serveur DNS Grenoble
  - Primaire grenoble.urec.cnrs.fr
  - Secondaire paris.urec.cnrs.fr et urec.cnrs.fr
- Serveurs DNS secondaires : Jussieu, Grenoble, …

UREC : messagerie

- Objectifs architecture
  - Adresses standards : Prénom.Nom@urec.cnrs.fr
  - Utiliser 2 serveurs (back up) : Paris et Grenoble
- MX urec.cnrs.fr ✍ Serveurs :
  - Mail.paris.urec.cnrs.fr (prioritaire)
  - Mail.grenoble.urec.cnrs.fr
- Alias par personne :
  - Jean-Luc.Archimbaud@urec.cnrs.fr ✍ Jean-Luc.Archimbaud@grenoble.urec.cnrs.fr
- Service accès aux boites aux lettres :
  - IMAP en local
  - IMAPS avec certificats électroniques à distance

UREC : autres services (pour l'UREC)

- **Web Intranet :**
  - **Contrôle d'accès par certificat**
- **Annuaire LDAP : interne**
- **Service listes de diffusion : SYMPA**
- **Multicast : routeurs configurés pour le recevoir**
- **NAT : pas utilisé**
- **Videoconf (actuellement téléconférence)**
  - **Etude pour l'achat d'un matériel H323 dédié (écran …)**
- **Administration**
  - **Un administrateur à Paris, un à Grenoble**
  - **Utilisation de BigBrother**

UREC : sécurité

- **Basée sur la segmentation et le filtrage**
- **Connexion vers l'extérieur**
  - **Tout est possible pour toutes les stations du personnel**
  - **Pour les autres (serveurs, machines tests, …) : limitée au maximum**
- **Connexion depuis l'extérieur**
  - **Vers certains serveurs locaux, depuis certains réseaux**
- **Filtres IP : aucun accès possible :**
  - **Extérieur ✍ ✍ machines tests, serveurs internes**
  - **Extérieur ✍ machines utilisateurs**
  - **Machines tests ✍ machines utilisateurs**
  - **…**
- **Filtres IP : accès restreints :**
  - **Extérieur ✍ serveur Web : uniquement Web**
  - **…**

UREC : sécurisation accès distants

- **Actuellement : n applications**
  - **Telnet, FTP, IMAP, HTTP vers Intranet**
  - **Sécurisation**
    - Filtrage : uniquement depuis certaines stations
    - Mot de passe ✍ SSL des applications (telnets, ftps, imps, https) avec utilisation des certificats électroniques
- **A l'étude : IPSec avec certificats électroniques**
  - **Station distante considérée comme station locale**
  - **Problèmes :**
    - Paramétrage de IPSec (fragmentation UDP)
    - Plus de débit nécessaire sur la liaison
    - Montages en tous sens demande bande passante
    - LA STATION NOMADE DOIT ETRE DE CONFIANCE
      - Pas d'autres connexions à l'Internet possible depuis cette station

Réseau de campus

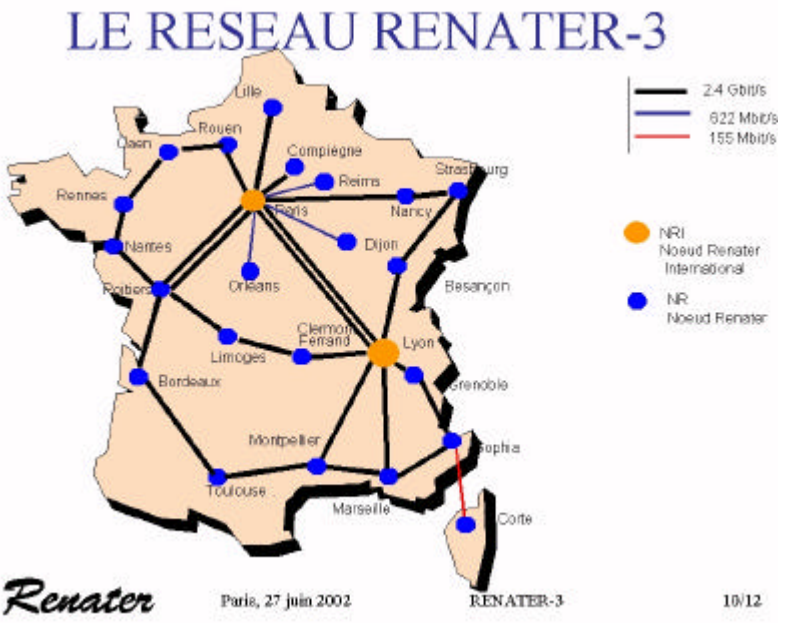
- **CNRS Meudon : 10 bâtiments**
- **Câblage :**
  - **Interconnexion FO**
  - **Intérieur des bâtiments TP Cat5**
- **Niveau 2-3**
  - **Cœur de réseau : commutateur 100 et GigaEth**
  - **A l'entrée de chaque bâtiment : routeur**
  - **A l'intérieur des bâtiments : commutateurs – hubs**
  - **Sortie vers Renater : routeur**
- **Adressage IP**
  - **3 classes C**

Réseau de campus : services

- **Messagerie**
- **Serveur Web**
  - **Internet**
  - **Intranet : contrôle d'accès par numéro IP**
- **Sécurité**
  - **Filtres sur les routeurs**
  - **Contrôle d'accès et traces sur les serveurs (tcp-wrapper)**
- **Equipe**
  - **2 ingénieurs**
  - **Groupe des correspondants de laboratoire**

RENATER : services

- **REseau NAtional de la Technologie, de l'Enseignement et de la Recherche**
  - **GIP : Min Ens Sup, CNRS, INRIA, CEA, …**
- **Service interconnexion IP**
  - **Réseaux région**
  - **Réseaux métropolitains (MAN)**
  - **Gros sites**
  - **Autres opérateurs français : GIX : SPHINX**
  - **Connexion internationale**
- **Autres services**
  - **IPv6**
  - **Multicast**
  - **VPN**
  - **CERT**

RENATER : architecture

- **Opérateurs**
  - **N opérateurs pour les liaisons (FO)**
  - **Principaux : TD et FT**
  - **Un opérateur pour l'administration des équipements actifs (routeurs) : CS**
- **Architecture**
  - **ATM (VC avec IP) ✍ IP sur SDH**
  - **VPN : VC ATM ✍ IPSec**
- **NRDs : Nœuds de raccordement**
  - **Locaux techniques avec routeurs**
  - **Dans sites en région**